IOT AND THE CLOUD: THE FUTURE OF A DIGITAL SOCIETY

Logica BĂNICĂ[1], Magdalena RĂDULESCU[2], Cristian ŞTEFAN[3]

[1] Faculty of Economics and Law, University of Pitesti, Romania,
olga.banica@upit.ro
[2] Faculty of Economics and Law, University of Pitesti, Romania
magdalena.radulescu@upit.ro
[3] Faculty of Engineering, Informatics and Geography, Spiru Haret University, Bucharest, Romania
liviu.stefan@yahoo.com

***Abstract**: The integration of Cloud Computing into Internet-of-Things (IoT) could solving heterogeneity problems with its devices, protocols and technologies. IoT Cloud-based platforms also offer reliability, scalability, and security features in terms of reduced costs. For building an IoT Cloud platform we proposed a three-layered model and we emphasized the functions of the Fog/Edge and Cloud Application levels, leveraging on Cloud Computing. Also, we described several platforms existing on IT market and we presented several pros and cons arguments for using IoT Cloud platforms in business, public administration and healthcare.*

Keywords: Internet-of-Things, Cloud platform, Microservices.

JEL Classification Codes: C88, O30.

1. INTRODUCTION

In the near future, the umbrella of the IoT (Internet-of-Things) will encompass all internet-connected devices that we use daily (laptops, smartphones, tablets, sensors and other smart things etc.), and that fact will induce considerable changes in the industry, transport, cities, academia, healthcare and living places.

Internet-of-things (IoT) can not limit the processing of information to an application domain or coverage area, and therefore its implementation will also depend on the evolution of other systems and technologies, the most significant being Cloud Computing.

In this paper, we focused on presenting these two concepts and the importance of their fusion in platforms targeting the business and social environment.

In our previous research we presented a three-layered IoT model (Physical, Fog / Edge and Cloud), the middle layer being hosted also using Cloud Computing technology on limited areas, and taking over some of the processing activities from the higher level (Banica et al., 2017a).

The literature offers several definitions for the IoT, all of them highlighting the role of smart device interconnection.

According to Rusu, the Internet of Things (IoT) is „the network of physical objects around us that contain electronic components, software, sensors and networking systems, situation that allows these objects to exchange and acquire information" (Rusu, 2017).

The International Telecommunication Union (ITU), in Recommendation ITU-T Y.2060, defined the Internet-of-Things as a "global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" ITU, 2012).

After a brief overview of the current evolution in this area (section 2), our paper aims to present methods and technologies for building IoT Cloud-based platforms, as well as a range of tools provided by important software companies (Section 3).

In Section 4, we will define a device-centric model of an IoT platform, outlining our pros and cons related to the building of such a system with free, open source software.

2. STATE OF THE ART

This section will provide a brief overview of the current studies and research regarding the concepts addressed in this paper, and especially IoT Cloud platforms.

The increasing number of smart objects that are connected to the Internet each day, determined by the technological advances in the mobile device industry, as well as the development of cloud-based integrated services, capable of collecting and processing large volumes of data and to perform complex reports, charts and predictive analytics, have led to a real revolution in the field of Internet of Things.

As the year 2019 is expected to bring the first commercial 5G implementations to the market, the industry is about to be transformed by the whole new level of interaction that smart devices will be capable of.

According to Ray, there are two main components that have contributed to the evolution of IoT, namely the Internet, which is "the backbone of the communication system to establish a smart interaction between people and surrounding objects", and the Cloud, which is the component providing "valuable application specific services in many application domains" (Ray, 2017).

From the beginning, IoT relied on Cloud computing capabilities in all of its forms, defined by National Institute of Standards and Technology - NIST (NIST, 2011): Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) and in time, the fusion of these concepts emerged to the term of IoT Cloud platform.

We summarized the services provided by each model described by NIST (NIST, 2011) (Banica et al., 2013):

- Infrastructure as a Service (IaaS) is the way to run one's applications and operating systems in the Cloud;
- Platform as a Service (PaaS): for even less burden on the client, the hardware and base software (operating systems, databases, and specialized middleware) are pre-configured and offered by the Cloud provider;
- Software as a Service (SaaS) implies that the whole software stack, including the hardware backend, are maintained by the Cloud host, giving the end-users the chance to interact with them on every available platform, be it desktop or mobile.

In the latest period, another model emerges on Cloud, IoT-as-a-service (also called IoTaaS) platforms, referring to services that define device functionalities and describe their connection to end-users and other things, and also to analytics of collected data.

Simmhan (2017) considers that IoT platforms could be implemented on the architecture presented in Figure 1, but with different points of focus:

- Cloud-centric - the focus is on the Cloud layer, data being stored and analyzed at this level, and also the Fog / Edge intermediate layer is managed from here, whose functionality is reduced;
- Device-centric (Fog/Edge computing): most part of the work is done in the Fog / Edge layer, data is collected and initially processed in nodes located near to devices, and the analytical part is performed by the cloud layer.

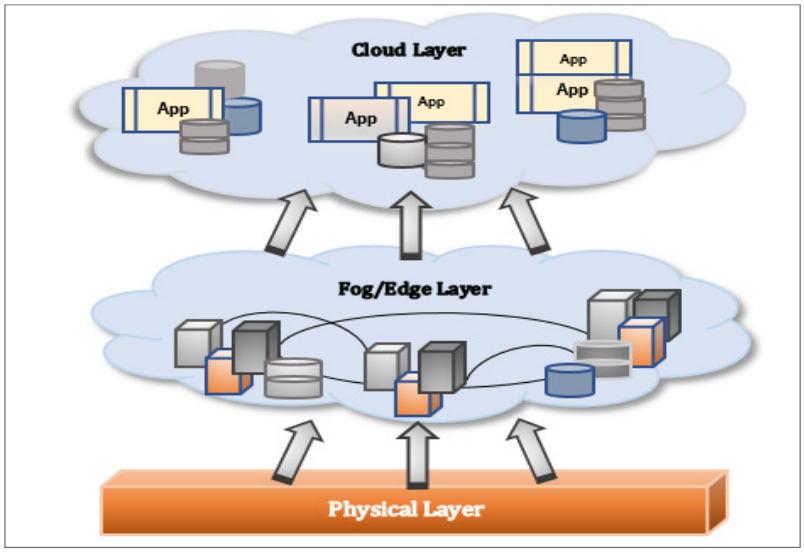

Fig. 1 The Cloud-based architecture of an IoT platform

Source: (Banica et al., 2017a)

The authors of this paper consider that Device-centric will be the most common approach, because it delivers decentralization, provides more flexibility and scalability, while increasing the management capabilities and the security.

The IT market offers many platforms that are able to host IoT solutions in any domain (business, education, healthcare, transport and telecom), some being open-source, and some having a commercial license. They are developed by the big players in this industry, such as: Google Cloud Platform, Microsoft Azure Cloud, IBM Blue Mix, Amazon Web Services, Oracle Integrated Cloud, Rackspace or OVH.

After reviewing and evaluating the open-source platforms available in 2017 and taking into account several criteria (like device management, protocols for data collection, analytics operatons, security), Rusu (Rusu, 2017) and other researchers made a prioritization.: KAA IoT platform, Particle cloud for Raspberry Pi, CARRIOTS IoT platform, Everything IoT platform, TEMBOO IoT platform.

In the following sections we will describe the components of an IoT Cloud-based platform and the implementation technologies, and finally we will highlight the pros and cons of implementing it in business environment.

3. METHODOLOGY

3.1 The role of Cloud computing for IoT development

Cloud computing is the technology that plays an important role in the development of IoT by providing a set of hardware and software products offered as on-demand services: processing, storage or shared network resources.

Cloud computing helps overcoming local hardware limitations by providing access to a common pool of configurable computing resources.

The companies' business model is defined by service requests that can expand and adapt to customer needs. Therefore, the Cloud represents the ideal environment for deploying user-to-machine and machine-to-machine communication applications, and offers the storage space required by the large amounts of generated data.

In addition, Cloud customers do not need to make investments for hardware, management platforms or other components of the IoT infrastructure, they can request subscription-based services, and the pool of allocated resources is tailored to their needs.

Regarding Cloud-based data storage, the traditional relational database organization model is heavily limited, and new database architectures, like the NoSQL concept, are purpose-designed for Big Data.

3.2 IoT Platforms

IoT platforms include a suite of components that manage smart objects using the data gathered from them, and analysed by applications designed as services in the Cloud infrastructure.

The IoT platform reference model includes two levels of Cloud processing, namely:

- Fog / Edge - an intermediate layer between Physical and Application layers, designed to deliver simple services to devices, to decentralize Cloud operations, and consequently to respond faster and more effectively to the demands of "things". This layer consists of several nodes that have their own storage and service capability. Simple functions attached to objects, such as connection and data transmission or receiving control signals, can be accomplished with the help of microservices, accessible via API gateways (Zhang, 2016). A device that requests a service will cause the creation and execution of a new instance of a microservice application with appropriate memory and CPU resources (Schone, 2017).
- Cloud Application layer – represents the environment where the centralized database (Big Data) is stored, used for deploying the complex operations, such as analytics, statistical, predictive and business intelligence.

There are many Cloud platforms launched on the IT market with different capabilities for IoT, such as Amazon Web Services IoT, Microsoft Azure IoT, Cisco IoT Cloud Connect and Google Cloud IoT, each offering various sets of IoT services.

The Amazon Web Services IoT is a monitoring system proposed to keep track of application performance metrics and to always have resource evidence through an agent placed on each service instance which informs about the evolution, events, specific instance data, until the session closes (Banica et al., 2017b). This information is stored in a unified database, in order to be used for analytics, create alerts or predict future trends (Jung et al., 2016).

The Azure IoT Edge platform, launched by Microsoft in 2017, allows "to connect to and interoperate with Cisco Fog deployments", meaning that the applications built and hosted in Azure IoT can be used at an extended scale through the Cisco fog platform (George, 2017).

Based on Cloud IoT Core, that allows easy and secure connections, managing data from devices, as Google Cloud IoT provides a set of tools to process, store, and analyze data both at the Edge or at the Cloud layer (https://cloud.google.com/solutions/iot/, 2018) (https://cloud.google.com/iot-core/, 2018).

The evolution of IoT platforms is aiming to the Internet of Things-as a Service (IoTaaS), offered to enterprises as a cloud platform for the development, customization and operation of IoT applications related to a business, accessible through a graphical user interface.

4. BUILDING AN IOT CLOUD PLATFORM

In this section we will present a device-centric IoT Cloud platform that we consider to be the most appropriate for running a business on a larger geographic area with multiple data collection and service delivery points.

4.1 IoT platform reference architecture

Building an IoT platform in the Cloud, implies the implementation of the following steps:

1) Defining the layered, device-centric IoT model with Fog/Edge computing as intermediate levels;
2) Specifying the services and applications running on the Fog/Edge and Cloud layers;
3) Defining the ways to access these services and applications, starting from bottom (devices) to the top of model (the complex data processing requirements).

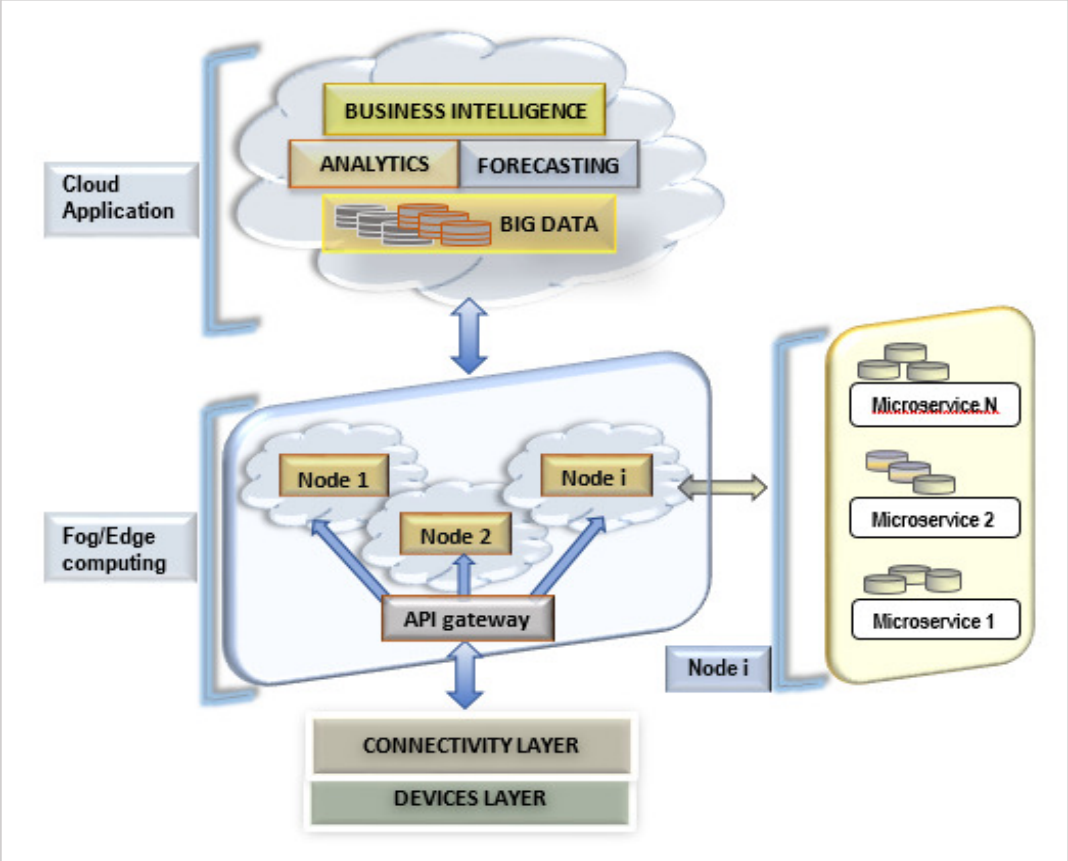

Fig. 2. A device-centric model of an IoT platform

(Source: Banica et al., 2018)

The distributed operations executed in the Fog/Edge nodes involve parallel pre-processing of the information (filtering, temporary storing, distributing and analysing sensor data) and forwarding the results to a centralized analytical processing application running in the Cloud. Also, they may be related to possible feedback received via control signals, as commands for the smart things.

The Fog/Edge layer stores structured and unstructured information into NoSQL databases, which can be processed by Hadoop in clustered platforms. This intermediate level is composed of nodes which run microservices, required by the devices connected via API gateways.

Application programming interfaces - APIs are communication points (method calls) and protocols that define a standardized interaction between devices and cloud computing resources, and allow applications deployment.

Although the Fog/Edge layer is essential for the IoT platforms, the most important operations are performed at the Cloud Application layer, and consist of aggregating structured and unstructured data (like social media) in Big Data collections, and its analytical processing to facilitate the decision-making process.

The third level - Cloud-based IoT platform - includes IoT's Big Data intelligent processing, consisting of analysis, filtering, and forecasting operations, carried out by business intelligence tools that lead to new information on which future decisions and management strategies are built upon.

Data and application security represent the main issue of the IoT platforms, a reason for which end users have not yet adopted this model on a large scale, and a key focus point for Cloud service providers.

4.2 Examples of IoT Cloud platforms

This section presents several of the best known IoT platforms, underlying their features in terms of functionality, advantages and drawbacks.

A) KAA - is an open source IoT platform proposed by the Apache Software Foundation to build smart, connected and end-to-end IoT solutions.

Its main features are (KAA project, 2018):

- relies on cloud computing and microservices
- allows data exchange between attached devices, data analysis, IoT cloud services monitoring
- works with SDK endpoints; an endpoint SDK is a library that provides communications, data collection, configuration profiles, and allows sending messages.
- back-end solutions include data security, consistency, interoperability, and data management with the SDK embedded in the developer's device.
- data storage is implemented with SQL databases like MariaDB and PostgreSQL, and NoSQL databases like Cassandra and MongoDB; the preferred open source software framework for storing and managing data is Hadoop. a Java based programming software, developed by Apache and used by many organisations, such as: Amazon Web Services, Intel, Cloudera and Microsoft.

According to Ray (2017), the main disadvantage of KAA is that it accepts fewer hardware modules than other platforms.

B) CARRIOTS is an end-to-end Internet of Things (IoT) platform, a Platform as a Service (PaaS) that offers scalability for projects, a quick adaptation to a growing number of devices, in terms of data collection and development of specific applications. The IoT solution encompasses Cloud High Performance Computing, Big Data analytics and Application Enablement Platform (AEP) technologies (CARRIOTS, 2013).

C) ThingsBoard is an open source, server-side IoT platform which distributes workload across multiple nodes. Each node is identical and can handle requests from both device and server-side applications.

ThingsBoard allows device management, data collection, processing and visualization for microservices. ThingsBoard adopts transport encryption and many types of device credentials, as security methods IThingsBoard, 2018).

4.3 Pros and cons about IoT cloud platforms

The actual Cloud platforms do not respect the standardized format of data representation. Security, communication and identification standards need to evolve to keep the pace with the widespread of IoT cloud technologies, whilst designing emerging technologies.

Also, other drawbacks refer to:

- the heterogeneity of "things" that interact through various communication technologies (Bandyopadhyay, 2011);

- incompleteness or inaccuracy of data, as a consequence of the increasing number of devices which exceeds the capacity of allocated resources,

- occurrence of security issues, like data security risks, cybernetic attacks of any kind, the risk of damage to the devices connected to the network etc.

The first malware for IoT was recorded in 2013, but in 2015 there was a powerful attack that infected connected devices, by accessing them based on default credentials (username and password), and using these devices for DDoS attack (Distributed denial of service) (Symantec site, 2016). These attacks have blocked several sites and hosting companies by flooding them with large amounts of traffic. Ironically, the malware code is available as open source for learning and implementing.

There are several solutions for the mentioned problems, such as: the standardization of device types and the communication protocols, increasing communication speed using 5G mobile networks, and multi-layer security applied across the whole ecosystem, from end devices to the Cloud application level.

Although it's a pretty new concept, many types of IoT applications have been launched, such as:

- supply chain management, like the tracking of goods exact location in smart warehouses and intelligent transportation systems;
- real-time monitoring of in-store sales, with continuous updating of stock-related information and live transmission to supplying warehouses
- intelligent shopping, consisting in the collection of consumer information and recommending items of interest, in accordance with its preferences
- implementing "smart buildings", where intelligent monitoring and control techniques are applied to all the systems within a building, in order to optimize their functioning performance
- developing "smart cities", by supporting citizens to get real-time information about public services and communicate efficiently with the public administration, find business opportunities and implement ecology-based behaviors, benefits that improve the quality of life
- intelligent medical applications, such as remote monitoring and treatment of patients, preventive care, improving diagnostics and medical performance.

5. CONCLUSIONS

Our work aims to achieve four objectives, namely:

- to describe terms like Cloud Computing and IoT, in order to define the new concept of IoT Cloud platform; Cloud is an efficient solution for connecting and managing a huge number of "smart things" in IoT, and also for storing the large amount of IoT-produced structured or non-structured data in Big Data platforms.
- to present an overview of the current state-of-the-art regarding the IoT Cloud platforms;
- to describe the device-centric model of the platform, underlying the design and functionality of the Fog/Edge and Cloud applications layers, and enhancement of the functions; using multiple nodes, the Fog/Edge layer collects data from the devices and implements quickly-accessible on-demand services by using a microservices-based architecture. The next layer aggregates data and provides important virtual processing capabilities for analytics, predictive algorithms and decision making.
- to present the features of some platforms already implemented on the IT market.

Integrating Cloud computing with IoT leads to a powerful synergy - Cloud-based Internet of Things, which offers processing power and storage, solving the security and performance issues and allows for the smart usage of devices in many real-life scenarios, in the business environment, smart cities, smart universities, intelligent healthcare and optimized energy management.

REFERENCES

1. Banica, L., Rosca, D., Radulescu, M., Hagiu, A., (2017a*) Internet-of-Things – A Layered Model for Business Environment*, Annals of "Dunarea de Jos" University of Galati, Economics and Applied Informatics, no3/2017, www.eia.feaa.ugal.ro
2. Rusu, L., D., (2017) *IoT Platforms: Analysis for Building Projects,* Informatica Economică journal, vol. 21, no. 2/2017, DOI: 10.12948/issn14531305/21.2.2017.04
3. International Telecommunication Union (ITU) (2012), Recommendation ITU-T Y.2060: Overview of the Internet of things, http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx
4. *Final Version of NIST Cloud Computing Definition*, (2011), NIST Special Publication 800-145, published on October 2011, available on http://www.nist.gov/itl/csd/cloud-102511.cfm
5. Banica, L., Stefan, C., (2013), *From Grid Computing to Cloud Infrastructures*, International Journal of Computers & Technology, Vol 12, No.1, pp. 3187-3194
6. Ray, P.P. (2017), *A survey of IoT cloud platforms*, Future Computing and Informatics Journal, Volume 1, Issues 1–2, December 2016, Pages 35-46, https://doi.org/10.1016/j.fcij.2017.02.001
7. Simmhan, Y., (2017), *IoT Analytics Across Edge and Cloud Platforms*, https://iot.ieee.org/newsletter/may-2017/iot-analytics-across-edge-and-cloud-platforms.html
8. Banica, L., Stefan, C., Hagiu, A. (2017b) Leveraging the Microservice Architecture for Next-Generation IoT Applications**,** Scientific Bulletin – Economic Sciences, Volume 16/ Issue 2, pp. 26-32
9. Meola, A. (2016), *What is the Internet of Things (IoT)?,* Business Insider, http://uk.businessinsider.com/what-is-the-internet-of-things-definition-2016-8?r=US&IR=T
10. Jung, M., Möllering, S., Dalbhanjan, P., Chapman, P, Kassen, C. (2016), *Microservices on AWS*, Amazon Web Services, Inc., https://d1.awsstatic.com/whitepapers/microservices-on-aws.pdf
11. George, S. (2017), *Microsoft and Cisco enable Azure IoT Suite to connect to Cisco Fog Deployments,* https://azure.microsoft.com/en-us/blog/microsoft-and-cisco-enable-azure-iot-suite-to-connect-to-cisco-fog-deployments/
12. Google Official site (2018) https://cloud.google.com/iot-core/

13. Google Official site (2018) https://cloud.google.com/solutions/iot/
14. Zhang, C. (2016), *Fog and IoT: An Overview of Research Opportunities,* IEEE Internet of Things Journal, doi:10.1109/EuCNC.2017.7980667
15. Schöne, P. (2017), *Developing for IoT Devices on The Edge*, http://www.iotevolutionworld.com/fog/articles/434967-developing-iot-devices-the-edge.htm
16. Banica, L., Polychronidou, P., Radulescu, M. and Stefan,C. (2018*), When IoT Meets DevOps: Fostering Business Opportunities* in *The Economies of the Balkan and the Eastern European Countries in the changing World*, KnE Social Sciences, pages 208-217,. DOI 10.18502/16
17. KAA IoT Development Platform (2018) overview available at: https://www.kaaproject.org/overview/26-10-2018
18. CARRIOTS technical presentation (2013) *Building an internet of things* Project available at: https://www.carriots.com/newFrontend/img-carriots/press_room/CARRIOTS technical_presentation.pdf
19. ThingsBoard Reference Documentation (2018) available at: https://thingsboard.io/docs/reference/pe-demo-getting-started/
20. Bandyopadhyay D, Sen J., (2011) *Internet of things: applications and challenges in technology and standardization*, Wirel Personal Commun 2011;58(1): 49-69.
21. Symantec official site (2016) available at: https://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks