Cloud-Based Cyber Physical Systems

Luca Brodo[1]

Contents

[1] luca.brodo@hshl.de

Abstract: The recent advancements in the area of cloud based solutions accelerated the development of Cyber-Physical Systems(CPS) that adopt cloud-based paradigms. Typically, CPS are limited in computation and storage due to their size and because they tend to be embedded into larger systems. The integration with cloud computing offers several new opportunities for CPS to extend their capabilities by taking advantage of the cloud resources. The adoption of these systems, however, still does not provide assurances on simultaneous quality of services, like timeliness, reliability and security, which are essential for CPS to operate in most cases. In this paper we will explore what cloud-based Cyber-Physical Systems are, their challenges and give an overview of the research efforts on the integration of CPS with cloud computing.

1 Motivation

Internet of Things (IoT) and Cloud Computing are the two most prominent information and communications technologies (ICT) and are integrated in a big variety of applications areas. IoT, which is said to be the future of the Internet [TW10], in which cyber-physical devices (or "things") are connected together through a network, extends the role of the internet from transporting pure, digital data to handling physical data emerging from CPSs. If the IoT paradigm brings a lot of new possibilities, there are still two major challenges that need to be addressed.[Ch16]

1. The processing of the large amount of data emerging from these devices, which do not have big computation and storage capabilities.
2. The seamless access to these devices by internet users through different channels.

Cloud computing represents the main solution to these problems since it provides the client with seamlessly unlimited computation power and storage.
In the last years there has been an increasing interest of integrating cloud computing solutions in with cyber-physical systems. [RR10]
There are three main reasons why this integration appears to be necessary.[Ch16]

Firstly, CPS devices are typically resource constrained with limited on-board processing and storage capacity. Adopting more advanced resources results in higher costs, which make CPS to expensive especially for large-scale applications. This results in the need for offloading computations from CPSs to much more powerful computers in the cloud.[Ch16]

Secondly, due to their own nature, CPSs are devices in continuous interaction with the physical environment around them collecting huge amount of data to feed back in the system. The analysis and the extrapolation of useful information from this data require a lot of computational power which makes the offloading process even more needed.

Finally CPSs are by nature also heterogeneous, which makes interoperability and transparency almost impossible. Virtualization of this resources expose them as services and facilitate their integration. From the above mentioned challenges, it is clear that CPSs have three main requirements:

- offloading intensive computation,.
- storing and analyzing large amount of data
- enabling seamless access through virtual interfaces

These are the major reasons why cloud computing represents a promising solution that addresses, and potentially solves, all these three challenges because, if coupled with a high-bandwidth connection to the CPS, it provides storage and computing resources as services to the back-end CPS, and allows for easier integration of these CPSs by virtualizing the access to them through standard Web service interfaces. [Ch16].
In this paper we will firstly explore why cloud computing enhances considerably CPSs. We will also discuss the main requirements, namely real-time processing, storage, and accessibility, as functional requirements, and security, as non functional requirements. In addition, this paper will explore some area of application, namely Cloud Robotics and Sensor Cloud along three axes: (1) computation offloading (or remote brain), (2) big data analytics, and (3) virtualization.

2 Cloud Computing foundamentals

According to the National Institute of Standards and Technology (NIST) , cloud computing *is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*.[NS]
In other words, cloud computing means that a third party application has access to all the applications and data in the system when the two are connected to the same network. The so called SService model"defines the type of resource this application can access and three service models are generally adopted:

1. Infrastructure as a Service (IaaS), where the hardware is available over the network.
2. Platform as a Service (PaaS), which provides a software environment where consumers can deploy their applications.
3. Software as a Service (SaaS), which offers a complete operating environment that contains management, applications, and the user interface.

These service models can be developed in 4 main ways:

1. Public Clouds: cloud services in public clouds are made available by a service provider for open, like Amazon AWS.
2. Private Clouds: are built for exclusive use of single client/organization
3. Hybrid Clouds: represent a combination of two or more distinct clouds to accomplish various functionalities within the same organization, like Google Cloud.
4. Community Clouds: represent a collaboration between several organizations to serve a common function or purpose.

A good design for a cloud computing service must be developed with different requirements in mind, but, for the sake of this paper, only Scalability, Reliability and Security will be mentioned.
Scalability implies that a cloud based application must be able to grow in size to accommodate increasing workloads from an increasing number of services connected to it. Scalability is strictly related to reliability, which means that the same scalable service must present a very low probability of either software or hardware failure.
Security, on the other hand, is essential in cloud computing because the service must be able to protect itself from attacks or attempts to steal sensible data.
Finally, one of the requirements which has not been mentioned before but is one of the most considered is obviously costs. As a matter of fact, the cloud-based service must be able to offer the most efficient service being as most cost effective as possible.

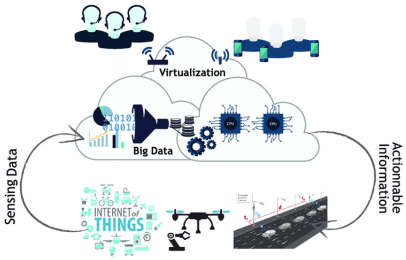

Fig. 1: Cloud based cyber-physical systems [Ch16]

3 Improvements brought by cloud-computing integration

Fig n. 1 gives a perfect overview of how CPSs can benefit from the adoption of cloud-based paradigms. The main idea is to empower the individual devices with web services, and enable them to participate in a service-based infrastructure. This is achieved by enabling them to (*i*) expose their functionalities as services, and (*ii*) empower them to discover and call other (web) services to complement their own functionalities.[SK10] This allows the cyber part in a cyber-physical system to be split into two different sub-parts, as show in Fig 2. Typical CPSs have two key parts integrated in balance, the physical part for interacting with the physical environment (e.g. composed of sensors and actuators), and the cyber part, which is the software part managing and enhancing the hardware of the CPS as well as its interaction with the environment. Thanks to the addition of another "cyber sub-part", namely the cloud one, the capabilities of the other on-device cyber parts can be expanded. In addition to expand the raw capabilities of the device in question, the manufacturer can also use such Cloud-based services in order to monitor the status of the deployed appliances, make software upgrades to the firmware of the devices, detect potential failures and notify the user, get better insights on the usage of his appliance and enhance the product, etc. [SK10]. In the following paragraphs, we will explore some fields in which cloud computing can greatly improve the performances of CPS.

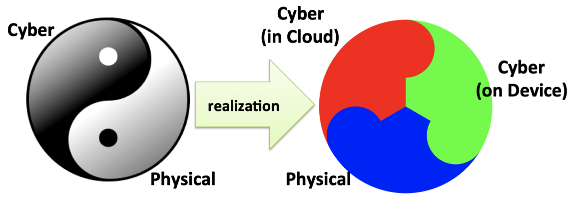

Fig. 2: Cloud-based Cyber-Physical Systems[SK10]

3.1 Real-time processing

Given their scope, CPSs must be capable of assuring a reliable service in a completely independent way. These systems, however, by design, tend to have stringent imposed constraints on performances which limit the execution of complex applications. Recalling that cyber-physical systems are typically real-time systems, in which, the application may be considered to have failed if it does not complete its function within the allotted time span and this may result in catastrophic consequences.
To circumvent this problem many have suggested to "contract out"the real-time processing to cloud platform. For instance, in paper [KS15] an IoT cloud platform for the connection of smart devices has been designed for real-time processing of data and control.In particular, they considered the deployment of robotics applications with strict processing delay and scalability requirements. The motivation behind this paper is that for some devices like sensors or small robots, only a small portion of data can be processed and only a small portion of this processes can be afforded in real time. The remainder must consequently be offloaded to a central server.

3.2 Storage

The rapid growth of the Internet of things has increased the amount of data generated from cyber-physical systems. These systems are now all over the world collecting data. Smarter vehicle management, home automation systems, surveillance, etc are all applications where cyber-physical systems generate a massive amount of data that should be stored somewhere for analysis.[Ch16] The exponential growth in the amount of data generated by cyber-physical systems needs a storage strategy that goes beyond the local storage solutions in the on-site system.
Memory and storage,along with communication, are fundamental performance metrics and energy bottleneck in these systems ([OM15],[MO15]). In the design of cyber-physical systems memory issues play a key role, and significantly impact their performance. Other than storing huge amount of data, CPSs' memory capacity needs to be able to scale with applications requirements. Unfortunately, this scaling exacerbate the weakness of storage capabilities in these systems. This represents an additional reason for the need to offload data and to some cloud solution.

3.3 Accessibility

The confluence of advances in wireless communication has lead to CPSs being deployed in applications where mobility is a necessity. The main example is vehicles, which they make an extensive use of CPSs, and they are in constant movements. This introduces additional challenges when it comes to protocol design and performance issues. The major challenge with mobile CPSs is that they might be inaccessible either permanently or intermittently if mobility support is not carefully addressed. [Ch16] Handoff and handover mechanisms are typically integrated in mobile network communication protocols to deal with mobility. Also in this case can cloud computing help to improve the effectiveness of these applications. For example, authors in [BK14] propose a mobility-aware trust worthy crowdsourcing framework in a cloud-centric IoT architecture. The framework incorporates user-mobility awareness while considering malicious alteration of data. They came to the conclusion that mobility-awareness and reputation-awareness in IoT application improve the effectiveness of smart city management authority.

4 Security and Safety

As discussed in the previous sections cloud computing paradigms improve CPSs in an innumerable ways, but brings along one potential major issue : security.
Cloud computing implies a network, which means that certain mechanisms must be put in place in order to assure correctness of the data, correctness of the result of computations, trust-ability of the nodes in the network, detection and control of unauthorized access and

recovery systems in case of an attack. These are ßtandard"problems in the network domain and well-established methodologies already exist to overcome them and assure security. CPSs networks are however a bit different from standard networks since, due to their nature, they are vulnerable to physical attacks and very sensible to physical-world irregularities and an attack at a physical level, through vandalism for example, has possible security consequences at cyberspace (or network level) and vice-versa. [Re14b]
The research world has already explored some of these issues, like intrusion detection[KP14] , emergency management [GW13] , and mathematical models [PDB13], and they are mainly achieved through sensor data. Trust-based packet transfer, agent- based trust calculation, and cooperative, collaborative approach for secure packet transfer are some of the examples of secure information transfer in sensor networks. [Re14b]
[GZM00] suggests various mathematical models to assure the affidability of a node in a network and these methods can be scaled to cloud-based CPSs. For example the Sporas formulae is used to test the trust of a node to transfer the packets in sensor network. It applies a reputation based system in which every node starts with a certain minimum reputation and this level varies during its activity on the system. After each transaction, the reputation values of the involved users are updated according to the feedback provided by the other parties to reflect their trustworthiness in the latest transaction.[GZM00]

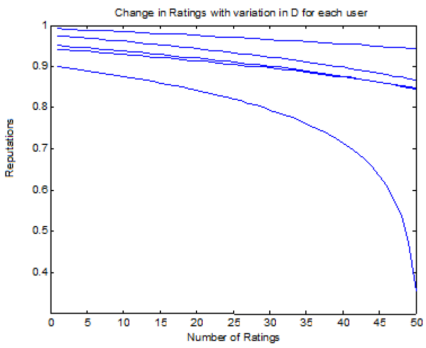

Fig. 3: Reputation of the nodes in a system calculated with sporas formulae [Re14b]

Sporas' equation implies also that the change in the reputation value of a user receiving a rating of W_i from user other other $\mathscr{R}_i$, is proportional to the reputation value $\mathscr{R}_i{}^{other}$ of the rater. In addition, since the reputation of a user in the community is the weighted average of non-negative values, it is guaranteed that no user can have a negative reputation value, thus no user can have a rating value lower than that of a beginner. Also, the weighed average schema guarantees that no user exceeds the maximum reputation value of 3000. [GZM00]
Fig n.3 shows the ratings of node A. The ratings of node A drops, while the ratings of other nodes stabilizes. The results show that the node A is in trouble (controlled by malicious activity) and requires further analysis (energy, the communication path, and other related

parameters). [Re14b]
The aforementioned interaction between CPSs and the real world environment is also a concern for safety: failures may escalate and impact it. In the context of Cloud-based CPSs, these systems are part of a large ecosystem and designing such systems with safety in mind is not trivial.
Having a secure CPS does not always mean that it is protected. In fact, a trade-off must be achieved to maintain both safety and security features in any CPS domain, where a safety feature is meant to protect the CPS from any accidental failure/hazard (system failure, miscalculations, abnormal activities, etc.), while a security feature (IDS, Firewalls, Artificial Intelligence (AI), etc.) ensures protection against intentional cyber-physical attacks.[M.20]
However, it is also worth mentioning that a fully implemented CPS technology with the network can increase safety dramatically. The potential of CPS improves in many areas including collision avoidance, air traffic control, robotic surgery, rescue operations, deep-see exploration, healthcare monitoring, and defense operations.It should not be considered a surprise that Cloud-based CPSs is one of the key areas of research in defense and civil operations.[Re14a] [Je17] provides a in-depth analysis on CPS security and privacy theory, guiding principles, and state-of-the-art applications. It also explores, the key technical, social, and legal issues at stake, and it provides readers with the information they need to advance research and development in area.

5 Example : Cloud Robotics

There has been an unprecedented effort in recent years to broaden the use of robot systems, as well as industrial robots, in other fields of application like smart home environments and smart office buildings [Ba07], airports [Ca07], labs,etc. Although robots have been proven useful for several scopes, their use is limited compared to other technologies such as smart-phones, mobile phones, tablets, etc. Essentially, robots have limited exposure to the general public at a large scale for the following reasons:

- Robots have been typically used as standalone systems for very specific and dedicated missions in controlled environments. Even in the case of cooperative and multi-robots applications, robots communicate with users or other robots to perform pre-defined tasks, yet are isolated from the external world.
- The complexity of modern robots make them a threat for the non computer-savvy users.
- Costs of maintenance and operation can be abhorrently high.

Given the above-mentioned limitations there is an increasing demand and interest in using the Internet infrastructure as a means of promoting robotics applications from two perspectives; by exposing robot resources as Internet services to end-users; and by enabling the robot-to-robot (R2R) as well as robots-to-end users communications through the Internet.

[Ch16] Robots may benefit from the cloud since it leverages the limitations of embedded hardware by enabling robots to offload computation and massive storage requirements to the remote cloud infrastructure which would be used as a ”remote brain”. Moreover, cloud-based solutions enable robots and humans to share and collaborate. In 2010, Kuffner [Me14] coined the term, ”Cloud Robotics” in his paper on Cloud-enabled robotics, providing a wide vision where robots can harness the massively parallel computation resources and vast data storage available via the networks. In the next sections we will briefly go through the three facets of Cloud Robotics: (1) Remote Brain: Offloading Computation, (2) Remote Storage: Big Data Processing, and (3) Remote and Distributed Collaboration.

5.1 Remote Brain: Offloading Computation

This has become in the recent years one of the most spoken topics regarding Cloud Computing in the research world. Robots may have limited on-board resources lending to stringent dimensional size and limited payload requirements, which means that they may not be able to carry on a relative big set of computational demanding tasks within the required timeline. In response to this, systems have been proposed that make a cloud service responsible for the computation of the the output from the inputs given by on-site robots. For example, [Pa10] describes a surveillance robot that require performing real time mapping, localization, autonomous navigation and object recognition. The robot can capture sensory data from its environment and send it to a cloud service, which permits running real-time processing tasks in parallel, including applications for video surveillance, image building using Point Cloud libraries (PCL), sensor information tracking, predicting and evaluating performance and other tasks. In the near future, robots would be used as actuating devices, capturing and offloading sensor data to the cloud infrastructure for rapid processing and analysis. Upon completion of the processed tasks, robots would actuate accordingly, driven by the response received from the cloud. [Ch16]

5.2 Remote Storage: Big Data Processing

One of the most talked-about topics in the industry and in academia is Big Data, both in terms of storage and in terms of processing. Given the inherent physical storage limitations in robots, especially the ones acting in the mobile field, providing access to remote cloud storage would allow robots to post sensor data, populate remote databases, help build and share knowledge bases, perform remote data analysis without the need for additional on-board memory. [Ch16] This leads to improved algorithms for robot path planning, object recognition, etc., leading to a collective intelligence space for robots to share. In respect to this idea several so-called knowledge databases have been proposed. For example, "Robo-Brain", [Un], is a projected ideated by the Cornell University to build a shared, large-scale knowledge base for robots to be able to function in human environment. This database allows robots to learn human's behavior and enables them to connect and learn from the robo brain knowledge-base instead of beginning from scratch.

5.3 Remote and Distributed Collaboration (Virtualization)

Sets of robots accessed remotely can collaborate together to perform various functions, tasks and sub-tasks to achieve unified goals. There are several issues and challenges that require attention, mainly: (i) Robot programming and manipulation is usually complex for beginners and naive users; (ii)monitoring and controlling robots usually rely on complex programming routines that cannot be handled by end-users; (iii) robots are typically expensive platforms and are not affordable for a large audience. [Ch16]
These challenges can be summarized by saying that a system which allows communications among robots is not very accessible due to costs and complexity. Like it usually happens in Computer Science, a solution for this problem is found in the concept abstraction. In fact, the virtualization of the whole systems allows to hide complexities and offers robot-as-a-service to the end-users. Virtualization is made possible by integrating cloud computing concepts in the system.

Authors in [Na12] present Jeeves, a distributed service framework for cloud based robot services. The key mechanism of the proposed framework is a robot assignment function, which discovers distributed robot resources and assigns the requested tasks by the users to suitable robots. Jeeves integrates various devices including robots with Internet services and provides a platform for offloading and executing computations in the cloud.

6 Conclusion

CPSs tend to be limited in terms of resources and they can not cope with the high demand of data they collect, both in terms of storage and in terms of computational power, i.e. they might miss deadlines and therefore not assure real-time results. Cloud computing seems to be the solution of these problems, even though it requires the engineers to focus more on safety and reliability. This paper explored the main benefits and challenges brought by the integration between CPSs and Cloud Computing and underlined the main security challenges with relative solutions found by other researchers.

7 Declaration of Originality

I hereby confirm that I have written the accompanying paper by myself, without contributions from any sources other than those cited in the text and acknowledgements. This applies also to all graphics, drawings, maps and images included in the paper. The paper was not examined before, nor has it been published.

Bibliography

[Ba07] Baeg, Seung-Ho; Park, J.; Koh, Jaehan; Park, Kyung-Wook; Baeg, M.: Building a smart home environment for service robots based on RFID and sensor networks. 2007 International Conference on Control, Automation and Systems, pp. 1078–1082, 2007.

[BK14] B. Kantarci, H. T. Mouftah: Mobility-aware trustworthy crowdsourcing in cloud-centric internet of things. IEEE Symposium on Computers and Communications (ISCC), 2014.

[Ca07] Capezio, Francesco; Mastrogiovanni, Fulvio; Sgorbissa, Antonio; Zaccaria, Renato: The ANSER project: Airport nonstop surveillance expert robot. IEEE International Conference on Intelligent Robots and Systems, pp. 991 – 996, 12 2007.

[Ch16] Chaâri, Rihab; Ellouze, Fatma; Koubâa, Anis; Qureshi, Basit; Pereira, Nuno; Youssef, Habib; Tovar, Eduardo: Cyber-physical systems clouds: A survey. Computer Networks, 108:260–278, 2016.

[GW13] Gelenbe, Erol; Wu, Fang-Jing: Future Research on Cyber-Physical Emergency Management Systems. Future Internet, 5(3):336–354, 2013.

[GZM00] G. Zacharia, A. Moukas; Maes, P.: Collaborative Reputation Mechanisms for Electronic Marketplaces. Decision Support Systems, 29(4):7–29, 2000.

[Je17] Jeschke., Houbing Song; Glenn A. Fink; Sabina: Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications. Springer, 2017.

[KP14] Karim, M.; Phoha., V.: Cyber-physical Systems Security. Springer, 2014.

[KS15] K. Supun, C. Leif, F. Geoffrey: A framework for real time processing of sensor data in the cloud. Journal of Sensors 2015, 2015.

[M.20] M., Yaacoub JA; Salman O; Noura HN; Kaaniche N; Chehab A; Malli: Cyber-physical systems security: Limitations issues and future trends. Microprocess Microsyst., 2020.

[Me14] Mester, Gyula: Introduction to Cloud Robotics. Conference: 32nd International Conference Science in Practice, SIP 2014, 10 2014.

[MO15] M. Onur, M. Justin, S. Lavanya: The main memory system: Challenges and opportunities. Communications of the Korean Institute of Information Scientists and Engineers (2015) 16 – 41., 2015.

[Na12] Nakagawa, S.; Igarashi, N.; Tsuchiya, Y.; Narita, M.; Kato, Y.: An implementation of a distributed service framework for cloud-based robot services. IECON 2012 - 38th Annual Conference on IEEE Industrial Electronics Society, pp. 4148–4153, 2012.

[NS] NSIT: , The national institute of standards and technology.

[OM15] O. Mutlu, L. Subramanian: Research problems and opportunities in memory systems. R, Supercomputing frontiers and innovations 1 (3)., 2015.

[Pa10] Paola, Donato Di; Milella, Annalisa; Cicirelli, Grazia; Distante, Arcangelo: An Autonomous Mobile Robotic System for Surveillance of Indoor Environments. International Journal of Advanced Robotic Systems, 7(1):8, 2010.

[PDB13] Pasqualetti, Fabio; Dörfler, Florian; Bullo, Francesco: Attack Detection and Identification in Cyber-Physical Systems. IEEE Transactions on Automatic Control, 58(11):2715–2729, 2013.

[Re14a] Reddy, Y: Cloud-Based Cyber Physical Systems: Design Challenges and Security Needs. Proceedings. 2014 10th International Conference on Mobile Ad-Hoc and Sensor Networks, 2014.

[Re14b] Reddy, Yenumula: Cloud-Based Cyber Physical Systems: Design Challenges and Security Needs. Proceedings - 2014 10th International Conference on Mobile Ad-Hoc and Sensor Networks, MSN 2014, 12 2014.

[RR10] R. Rajkumar, I. Lee L. Sha J. Stankovic: Cyber-physical systems: The next computing revolution in: Design Automation. 2010 47th ACM/IEEE, 2010.

[SK10] Stamatis Karnouskos, Armando W. Colombo, Thomas Bangemann: Trends and Challenges for Cloud-based Industrial Cyber-Physical Systems. Industrial Cloud-Based Cyber-Physical Systems, 2010.

[TW10] Tan, Lu; Wang, Neng: Future internet: The Internet of Things. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 5:V5–376, 09 2010.

[Un] University, Cornell: , The Robo-brain project.