Available online at www.sciencedirect.com
ScienceDirect
Procedia Computer Science 97 (2016) 135 – 139
Procedia Computer Science

CLOUD FORWARD: From Distributed to Complete Computing, CF2016, 18-20 October 2016, Madrid, Spain

Cloud challenges towards Free Flow of Data

Erkuden Rios[a,]*, Massimiliano Rak[b]

[a]*Tecnalia, Parque Científico y Tecnológico de Bizkaia, C/ Geldo, Edificio 700, 48160 Derio, Spain*
[b]*Seconda Università degli Studi di Napoli, Via Roma 9, 81031 Aversa, Italy*

Abstract

The Free Flow of Data is an emerging challenge to which the European Commission is currently working on with a legislative proposal due for the end of 2016, as part of the Digital Single Market (DSM) strategy. The proposal aims at tackling unjustified "restrictions on the free movement of data" among Member States. This paper analyses a number of cloud challenges of trustworthy inter-cloud environments identified by on-going EU-funded research initiatives dealing with security, privacy and data protection issues of Cloud solutions.

Peer-review under responsibility of organizing committee of the international conference on cloud forward: From Distributed to Complete Computing

Keywords: security; privacy; inter-cloud; free flow of data

1. Introduction

The European Commission is currently working on a legislative proposal on Free Flow of Data (due for the end of 2016), as part of the Digital Single Market (DSM), i.e. the Pilar I of the Europe 2020 Strategy[1]. The proposal aims at tackling "restrictions on the free movement of data for reasons other than the protection of personal data within the EU and unjustified restrictions on the location of data for storage or processing purposes. It address the emerging issues of ownership, interoperability, usability and access to data in situations such as business-to-business, business

* Corresponding author. Tel.: +34 946 430 850.
E-mail address: erkuden.rios@tecnalia.com

Peer-review under responsibility of organizing committee of the international conference on cloud forward: From Distributed to Complete Computing
doi:10.1016/j.procs.2016.08.291

to consumer, machine generated and machine-to-machine data. It will encourage access to public data to help drive innovation"[1].

These restrictions are likely limiting the Single Market for cloud-based applications and cloud services, among others. According to the estimates in "SMART 2013/0043 - Uptake of Cloud in Europe" report[2], in year 2020, cloud computing business could reach €103b of net new GDP (including the public sector), a share of 0.71% of total EU GDP. Therefore, the Free Flow of Data is seen as a key enabler of the EU Data Economy growth in future years.

Other important cloud aspects such as certification of cloud services and switching of cloud service providers are in close relation to the Free Flow of Data and will also be tackled within the European Cloud Initiative to be launched by the Commission.

This paper analyses a number of cloud challenges of trustworthy inter-cloud environments which will be one of the architectural pillars of cross-border services in the Single Market. These challenges are those identified in the context of the collaborative activities of the DPSP Cluster[3], as explained in Section 2.

2. Methodology

The work presented in this paper was born from the activities of the Data Protection, Security and Privacy Cluster of EU-funded research projects on Cloud[3], a collaborative initiative made of 24 projects that work towards innovation on Cloud security and privacy. The clustered projects include mostly on-going H2020 projects but also a few FP7 projects and CIP projects. The DPSP Cluster, through a survey made among all the clustered projects, produced a whitepaper[4] which collects the research challenges that individual projects have identified with respect to the main areas of work of the Free Flow of Data (initiative #14 within the Digital Single Market strategy). It is worth noticing that some challenges proposed in the whitepaper have significant overlaps, due to the different source of information.

While the whitepaper collects the information on the challenges by project and topic, and the timeframe of the projects span from year 2016 to 2020 and beyond, in this paper we focus on all the challenges for the period of 2018-2020 that address the specific topic of *free movement of data*, trying to identify the open challenges that may affect the movement of data. For each challenge we propose our own interpretation of how it relates to and impacts the free movement of data.

According to the collected data, we conclude the paper with a brief summary of the challenges associated to the topic of free movement of data and our conclusions on the topic.

3. Free Movement of Data: The open Challenges

According to the DPSP whitepaper the main challenges related to free movement of data are briefly summarized in the following table, where we outline the relationship with the topic of *free movement of data*. For a detailed description of the challenge, we refer to the DPSP whitepaper[4]. In order to facilitate the references, for each challenge proposed we report the name of the source project that identified it.

Table 1. Open challenges for Free Movement of Data

#	Challenge	Relationship with Free Movement of Data	Keyword	Proposed by
1	Making the cloud ecosystem secure for outsourced data	The trust in Cloud Service Provider (CSP) is the key topic to enable easy movement of data.	Trust in CSP	CLARUS[5]
2	Privacy-enabling mechanisms to protect sensitive data	Customers need tools to control the protection of their data.	Privacy, Monitoring	CLARUS
3	Data protection and legal jurisdiction	Legal jurisdiction affect the security requirements of the applications, different laws imply different security requirements.	Law & regulation framework.	CLARUS
4	Interoperability-by-design to	Interoperability among CSP is the main	Interoperability	CLARUS

	overcome mistrust in cloud computing by implementing standardized cloud services	need to enable movement of data.		
5	Data flow control	Control access and usage of data in the whole flow.	Monitoring	COCO CLOUD[6]
6	Control of privacy conditions and obligations and adherence to them	Customers needs tools to control the protection of their data	Privacy, Monitoring	COCO CLOUD
7	Risk assessment frameworks for applications at scale	Risk management must be based on evaluation and not on perception to simplify and enable data movement	Trust in CSP, Security Quantitative Evaluation	MUSA[7]
8	Dynamic benchmarking and brokering of Cloud offers	Trust in CSP needed to move data should be continuously evaluated	Security Quantitative Evaluation	MUSA
9	Composition of evolving security-aware Service Level Agreements (SLAs)	Security SLAs are the way to assess trust in a clear and measurable way.	Trust in CSP, SLA, Security Quantitative Evaluation	MUSA
10	Fully secure API	APIs should be designed in a way to grant security requirement when data are being moved.	Trust in CSP	PAASWORD[8]
11	Searchable Encryption	Access and search data, respecting confidentiality and integrity of data enable the trust in CSP needed to grant movement of data.	Trust in CSP	PAASWORD
12	Authenticity and verifiability of data and infrastructure use	Security SLAs are the way to assess trust in a clear and measurable way.	Monitoring	PRISMACLOUD[9]
13	Simpler contractual terminology and commonly used taxonomy	Security SLA are the way to assess trust in a clear and measurable way.	Trust in CSP, SLA	SLA READY[10]
14	Standardisation and transparency in SLAs	Security SLAs are the way to assess trust in a clear and measurable way.	Trust in CSP, SLA	SLA READY
15	User-centric Security SLA Negotiation	Security SLAs are the way to assess trust in a clear and measurable way. Cloud Service Consumer (CSC) should be able to negotiate the security level and access providers according to such requirement.	Trust in CSP, SLA, Security Quantitative Evaluation	SPECS[11]
16	Security SLA Automatic Implementation	Security SLAs are the way to assess trust in a clear and measurable way. Automated SLA implementation will grant the right SLA when data are being moved from different CSPs.	Trust in CSP, SLA	SPECS
17	Security SLA Monitoring	To grant the right level of trust it is needed to concretely monitor the respect of the granted levels of security.	Trust in CSP, SLA, Monitoring	SPECS
18	Secure interoperable authentication in cross-border scenarios	Authentication among different sources and agreements on identity is needed to grant free flow of data.	Trust in CSP	STRATEGIC[12]
19	Definition and enactment of fine-grained security policies	Enabling the access to data according to specific policy in clouds supports the right Trust in CSP to enable free	Trust in CSP, Controllable	STRATEGIC

		movement of data.	policies	
20	Protected data sharing for federated clouds	Enabling the access to data according to specific policy in federated clouds supports the right Trust in CSP to enable free movement of data.	Trust in CSP, Controllable policies	SUNFISH[13]
21	Security and privacy terms in SLA Negotiation	Security SLA are the way to assess trust in a clear and measurable way.	Trust in CSP, SLA	SWITCH[14]
22	SLA transmission security	To grant the right level of trust it is needed to secure the SLA negotiation process too.	Trust in CSP, SLA, Monitoring	SWITCH
23	Privacy-preserving analytics/processing over confidential and efficient outsourced databases.	Customers need tools to control the protection of their data.	Privacy, Monitoring	TREDISEC[1][5]

4. Inter-cloud security and privacy challenges towards Free Flow of Data

In section 3, we analyzed the main challenges (23 in total) related to free movement of data proposed by the clustered security projects. According to such analysis we noticed that such challenges address mainly the following topics that are the ones that may really affect the free movement of data among Member States and in cross-border services: Trust in CSP, SLA Monitoring, Quantitative Evaluation, Privacy, Controllable Policies, Interoperability, Law and Regulatory framework.

Most part of the challenges proposed (15 challenges out of 23) explicitly address the problem of Trust in CSP. Probably this is the most limiting factor in a free movement of data: customers have a limited trust in CSPs, mainly due to the perceived lack of control over their data due to the nature of cloud paradigm. Free movement of data needs a clear solution to address such lack of trust and the possible approaches, outlined by the different challenges that the projects outlined and the approaches that they propose can be summarized in few topics: i) clear Service Level Agreements (SLAs), ii) Quantitative Evaluation of the clauses of the SLA and iii) automatic Monitoring and assurance. All together put the focus on how the security and privacy-aware behavior of the service is specified at requirements and SLA level and further monitored and controlled at runtime. The Service Level Agreements (outlined in 8 challenges out of 23), which are contracts among CSPs and CSCs on the quality of the services offered, look the way to clearly state the security requirements to be granted. They are strictly related to Monitoring and Quantitative Evaluation topics, i.e. the needs for solutions that enable to concretely measure security and privacy.

The need for tools able to offer to customers the capability to control security policies and or the usage of their data is the other way round to face the topic of Trust in CSP, i.e. enhance the capability of customers to control the data movements in the cloud environment through tools that demonstrate the actual usage of resources and access to the data stored or processed in such an environment.

It is worth noticing that interoperability is considered one of the key challenges, but it is proposed only in 1 out of the 23 challenges, and, therefore, it seems to be a factor addressable with existing technologies or not explicitly the focus of any of the clustered projects.

Acknowledgements

We thank all the authors of the Data Protection Security and Privacy in Cloud Cluster's "Whitepaper on Challenges for trustworthy (multi-)Cloud-based services in the Digital Single Market"[4] for creating the valuable input that led to this work.

References

1. The Digital Single Market (DSM), Available at: http://ec.europa.eu/priorities/digital-single-market_en, retrieved June 2016.
2. Final report SMART 2013/0043 Uptake of cloud in Europe, Available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9742, retrieved June 2016.
3. DPSP Cluster Web Site, https://eucloudclusters.wordpress.com/data-protection-security-and-privacy-in-the-cloud/
4. DPSP Cluster, "Whitepaper on Challenges for trustworthy (multi-)Cloud-based services in the Digital Single Market", Available at https://eucloudclusters.files.wordpress.com/2015/05/dpspcluster-whitepaper-v3-1.pdf
5. CLARUS project website, http://www.clarussecure.eu/
6. COCO CLOUD project website, http://www.coco-cloud.eu/
7. MUSA project website, http://www.musa-project.eu
8. PAASWORD project website, https://sites.google.com/site/paaswordeu/
9. PRISMACLOUD project website, https://prismacloud.eu/
10. SLA READY project website, http://www.sla-ready.eu/
11. SPECS project website, http://www.specs-project.eu
12. STRATEGIC project website, http://www.strategic-project.eu/
13. SUNFISH project website, http://www.sunfishproject.eu/
14. SWITCH project website, http://www.switchproject.eu/
15. TREDISEC project website, http://www.tredisec.eu/