PERSONAL DATA IN CLOUD. RUSSIA EXPERIENCE

Anna Zharova, Vladimir Elin & Petr Panfilov

* Director of Centre for Cyberspace Research, Associate Professor, Docent,
National Research University Higher School of Economics, Moscow

** Department of Information Security, Associate Professor, National Research University,
Higher School of Economics, Moscow

This Publication has to be referred as: Zharova, A[nn]a; Elin, V[ladimir] & Panfilov, P[eter] (2017). Personal Data in Cloud. Russia Experience, Proceedings of the 28th DAAAM International Symposium, pp.1136-1142, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-11-2, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/28th.daaam.proceedings.158

Abstract

The use of cloud computing to ensure interaction between the state and citizens allows to speed up information interaction, to realize state services, to reduce the costs of providing such interaction, but at the same time this interaction raises important questions about the reliability of the cloud provider and security of interaction. Providers of the cloud can be both public authorities and private organizations. In the event that the cloud provider is a government agency, it can be assumed that all the requirements for security will be met. However, if the cloud provider is a private person, then we cannot be sure of security, if these requirements for security are not mandatory. It should be noted that Russian legislation does not require the mandatory application of information security standards. In this regard, the security of stored information in the clouds and its legislative support, the responsibility of providers providing cloud access services are very significant for the use of this technology in Russia.

Keywords: cloud computing; the cloud provider; security; personal data; Russian legislation; cloud access services

1. Introduction

1.1. Main issues of this article

The term «cloud computing» is often used in various spheres of public life. «Cloud computing» refers to technology, which is created to optimize business processes and improve the service quality, different service providers and to increase people's informatization level. Questions on people's interpersonal relationship are arising more often in the field of medicine, government, the banking and private sector. The application of cloud computing is a strategy important development for the computer technologies and provides different services.

The active introduction of cloud computing (CC) put questions to the legislator about the specifics of regulating these people's behavior online. These are questions of data security when it is stored in the cloud computing and question

of whether the cloud computing is private or government owned. Question as to the requirements for the cloud Internet Service Provider's (ISP) effective functions as well as ISP's responsibility for it is own action and those of third parties, remain unanswered. Is it possible to be sure that technology which allows us access to the cloud computing is reliable and safe? What if public information and IT systems are hosted abroad?

Whether the government has determined the requirements for ensuring the security of information and emerging relationships the proper regulation and trust of citizens to the security of relationships depends.

The authors of this article will try to answer these questions.

1.2. Definition "cloud computing" in Russia

The State Program of the Russian Federation «Information Society (2011-2020)» [4] considers the development of cloud computing to be one of the main priorities. The creation of a national platform of cloud computing is provided in this government program. It is planned to connect all the public authorities of the Russian Federation in the period of 2011-2020. In 2010 to a Russian platform, the Deputy Minister of Ministry of Communications and Mass Communications of the RF said that «these kinds of proprietary technologies in Russia are practically absent therefore, this sector is actively engaging with foreign companies such as Google» [25].

Despite the active application of the term «cloud computing» in the Russian Federation, this term has no legislative definition. Despite this, «cloud computing» was taught at technical universities in 1990s and the further development of this technology at public institutes was predicted. Consequently, we used to definition which the Institute of Electrical and Electronics Engineers (IEEE) gave. According to the IEEE's definition published in 2008, «Cloudy data processing is a paradigm within which information is constantly stored on servers on the Internet and is temporarily cached with the client party, for example, on personal computers, game consoles, laptops and smartphones».[14] The IEEE, investigating the prospects of developing cloud computing drew a parallel between this technology and the Internet. In Russia, the following IEEE companies operate in Siberia, Northwest (St. Petersburg) and Central Russia (Moscow)[15].

The Strategy of the development of the information society in the Russian Federation for the years 2017-2030[10] defines the notion of "cloud computing" as an model of information technology, by use of the Internet, for ubiquitous and convenient access to a common set of configurable computing resources ("cloud"), data storage devices, applications and services which can be quickly provided and freed from the load with minimal operating costs or practically without the participation of the provider. Cloud computing is considered to be a platform, which provides various different services.

However, it is only classified in the technical sphere, and so the following classification of cloud computing is accepted:

1) SaaS (Software as a service) – in this case the user of cloud computing is granted the right to use and access the necessary software.

2) IaaS (Infrastructure as a Service) – the user of cloud computing is granted the right to use the provider's hardware-software complex for work and data storage.

3) PaaS (Platform as a Service) – the user of cloud computing is granted the right to use a hardware-software complex for to development, testing, expansion and support of web applications.

On 2013, the Russian Federation service for technical export control (FSTEC) set out project the State standard which defined the cloudy services such as:

- Hardware as a service (HaaS);
- Safety as a service (SecaaS);
- Business process as a service (BPaaS);
- Data as a service (DaaS);
- Trust as a service (TaaS);
- Infrastructure as a service (IaaS);
- Cloud development environment as a service (CDPaaS);
- Communication as a service (CaaS);
- Platform as a service (PaaS);
- The connection as a service (CnaaS);
- Transparency as a service (TraaS);
- Workplace as a service (WaaS).

In this article we will not consider the questions of processing of the state secrets or publicly accessible data by the CC. Of course, answers to the above questions are linked to category owner of cloud, whether they are a state or individuals, so cloud computing depending on the subject to whom they belong, can be public or private. Public clouds belong to the state authorities or the local council.

Furthermore, public cloud data may be better protected than the private cloud computing. The cloud technology can belong to foreign or Russian ISPs. Information can be public or have limited access (ch.2 Art. 5 of Federal law «Information, Informational Technologies and Protection of Information»). Limited access information can be personal data, «know-how» and secrets data importation from companies, and is regulated only by the Federal legislation.

2. Legal regulation on use of personal data in Russia

In 2014, a Russian Advisory council from the Ministry of Telecoms and Mass Communications was created to improve the development and implement a state policy and standard and legal regulation of cloud computing. The Advisory council aimed to develop suggestions for improving the legislation for cloud computing; ensure the regular interaction of the Ministry of Telecoms and Mass Communications with the expert community on cloud technologies.[2].

Experts in the technical sphere claim that it is impossible to ensure the absolute safety of these technologies. [18] Noriswadi Ismail has also written about these problems. [21], P.250]

We consider the difficulties that legislation encounters when trying to ensure the protection of limited access data, such as personal data[19]. As Angela Adrian remarks, "how should legal rules change to accommodate the new communication technology? If cloud computing does not alter our fundamental values, how should legal rules adapt and change in order to maintain our current values? What should the substance of our rules be in light of the changing environment for the actors in the cloud? [17], P.49]

According to Art. 7 of the Russian Federal law «On personal data» [5] «the operators of personal data and other persons who accessed to personal data are obliged not to disclose this information to third parties and not to impart personal data without consent of the subject of personal data . The other cases must be provided by the law».

What ought to be done if information is stored in a foreign cloud?

According to item 11. Art. 3 of the Federal law «On personal data» the cross-border transfer of personal data is the transfer of personal data to the territory of the foreign state, to the authority of the foreign state, to a foreign national person or the foreign legal entity.

Therefore, we can understand the cross-border transfer of personal data as the transmission of personal data of any person from the Russian Federation to a foreign person abroad. For example, when any person is filling in a form online to purchase goods from a foreign seller.

Art. 19 of the Law «On personal data» states that the Russian operator of personal data has to establish in the agreement with the foreign handler of the information, the duty to comply with the confidentiality of personal data, to ensure to safety of personal data, and also to comply with other requirements to protect the personal information. According to item 3. Art. 12 of the Law «On personal data» the operator of personal data must be convinced that the foreign country to which the data are transferred provides an adequate protection of the people's rights to their personal data. The Federal law «On personal data» specifies that states can be submitted as two groups of countries:

- 1) Member countries of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (1981); (This Convention came into force in the Russian Federation on September 1, 2013) [11]
- 2) Countries which are not the party to the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (1981), but which are listed as foreign states which provide adequate protection of the people's rights to their personal data. This is such countries¹.

The Russian Ministry of Telecom and Mass Communications in unofficial letter on May 13, 2009 explained that «the adequacy of protection means that foreign state provides the level of security of people's rights to their personal data, not below the standards provided in Russia. One of the assessment criteria of the state in this aspect is ratification of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (1981)» [12]

However, if the cross-border transfer of personal data is being carried, out in foreign states which are not providing adequate protection people's rights to their personal data, then the operator of personal data must receive, in written form, that consent person's for their personal data to be transferred. This relationship between foreign ISP (operator of personal data) and the owner of personal data is regulated by two the Russian laws. They are the Federal law «On personal data» and the Federal law «On electronic signatures». [7]

Accordance with part. 4 Art. 9 of the Federal law «On personal data» the participants in the relationship have the right to use an electronic signature to create a written form of their agreement. Art. 4 of the Federal law «On electronic signatures» defined the rights of parties in the electronic interaction to use any information technology and (or) the technical means, to apply an electronic signature. However, the Federal law «On electronic signatures» requires that participants (operator of personal data and the owner of personal data) must approve of these actions. This approval can be placed on the main web page of the cloud operator which handles personal data (ISP of personal data) on the conditions of using the type electronic signature and the technologies. The subject of personal data must agree with these conditions.

Although, there is another opinion, Kanashevsky V. writes that sending an e-mail message of the Russian's users to the foreign cloud ISP's of personal data no is electronic document signed the electronic signature. «The foreign operator potentially can be brought to civil liability in accordance with Russian law. In connection with this action, the claim for the damages and compensation for moral damages can be brought to the foreign operator. (Art. 17 of the Federal law «On Personal Data»). [20]

¹ Australia-Australian alliance; The Argentine Republic ; The State of Israel; Canada ; Kingdom of Morocco; Malaysia; United Mexican States ; Mongolia ; new Zealand; The Republic of Angola ; The Republic of Benin ; The Republic of Cape Verde ; The Republic of Korea ; The Republic of Peru ; The Republic of Senegal; Republic of Tunisia; Republic of Chile; Hong Kong Special Administrative Region of the People's Republic of China ; The Swiss Confederation // The Order of the Federal Service for Supervision of Communications, Information Technology and Communications of March 15, 2013 № 274 "On approval of the list of foreign countries that are not parties to the Convention of the Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data, and provide adequate protection of human subjects personal data" // <http://www.garant.ru/products/ipo/prime/doc/70268490/#ixzz3E8YwESIQ>

This opinion is erroneous. Firstly, the Federal law «On electronic signatures» points directly to the recognition of foreign electronic signatures. Article 7 of this Federal law indicated that «if the electronic signature is created in accordance with the law of a foreign state and the international standards then it is being recognized in the Russian Federation as the electronic signatures of the type which correspond the Federal law «On electronic signatures». Also, according part 2 of Art. 7 of the Federal law «On electronic signatures» an electronic document signed by electronic signatures cannot be regarded as illegal only on the basis that the key's certificate of the electronic signature verification is issued in accordance with the rules of the foreign law. [7]

Secondly, part 2 of Art. 9 of the Federal law «On personal data» determines that consent of the subject of personal data can be given in any form which allows officially confirm receiving this consent.

Thus, the Federal law «On personal data» and the Federal law «On electronic signatures» define the legal conditions of recognition the consent.

However, be aware that Federal law «On personal data» allows to the ISP (operator) of personal data to not obtain the consent of the subject of personal data if cross-border transfer of personal data is carried out «for the execution of the contract. And party to this contract is the subject of personal data (person) » (part 4 Art. 12 of the Federal law «on Personal Data »). Thus, this Federal law indicates the presence of the preliminary agreement on cooperation.

In addition, there is one additional exception by which the telecom operator does not have to obtain the consent of the subject personal data. So, in 2013, the Russian Federal law «On communications» was changed [8] [Federal law «On Communications»]. Art. 53 of this law was added the right of the telecom operator This right allows to the telecom operator entrust the processing of personal data to third parties without received the consent of person on this. But only, if the telecom operator processes the parties' personal data in according with contract for the provision of telecommunications services. And (or) the telecom operator acts for the implementation of the rights and legitimate interests of the service provider or the citizen. However, the Federal law «on Communications» did not disclose whether the operator must warn of the fact that personal data was processed by a third party.

Thus, the opinion about the complexities of the processing of personal data by the foreign cloud ISP (or operator of personal data) is a fallacy in most cases.

In 2013-2014, the total transmission model (provision) of personal data to external operators was changed in Russia. Expanded the list of cases in which the consent is not required of the subject of personal data on processing his data by third parties.

3. Ensuring the technological security of the transmission and processing of personal data.

Of course, the cross-border transfer of data is associated with problems of the ensuring the technological security of the transmission and processing of personal data. However, here it is necessary to take into account the opinion of technical experts, who believe that there are no absolutely safe technologies. Furthermore, there is a problem of difficulty of selecting a required standard of the existing standards. For example, in the report of the Europe Commission are indicated a problem of the difficulty in the selection of standards: «a jungle of standards generates confusion by, on one hand, a proliferation of standards and on the other hand a lack of certainty as to which standards provide adequate levels of interoperability of data formats to permit portability; the extent to which safeguards are in place for the protection of personal data; or the problem of the data breaches and the protection against cyberattacks...» [27]

But here it is necessary to bear in mind that there is no legal prohibition on the choice of the standards on the territory of the Russian Federation countries. The Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) of the Russian Federation accepted the «Methodical recommendations on the choice of methods of depersonalization of personal data». [16] In this methodical recommendations are submitted various methods to anonymize personal data. In case the depersonalization of personal data, the complexity of the selection standards is eliminated.

Providers of cloud services must address the questions of data security. Technological complexity of security in the cloud is that the virus-infected file from one client allows to infect this virus other connected and non-performing clients. In connection with this, there is the danger of cracking data is stored in the cloud. The responsibility for protection lies on the provider. Users of cloud services need to be sure that the provider is using security tools that reduce the likelihood of offending. The provider of cloud services should allow the user to check the level of protection and should to record the actions of all actors who have gained access to the cloud.

If there are no special requirements of the law, an owner of cloud computing can voluntarily be audited and certified by the ISO / IEC 27001: 2005 and (or) SAS 70 Type II and Type I.

The European Network and Information Security Agency (ENISA) proposed using ISO27001. Moreover ENISA pointed out that «all suppliers must demonstrate compliance. They are NOT required to be accredited but compliance is verified through yearly submission of their information security management system and associated policy documents.

In Russia, according to the Order of the Government of the Russian Federation of 22.02.2012 №238-p OJSC «Rostelecom» appointed as the sole executor for the further creation and development of complex information technology and telecommunications infrastructure and e-government for 2012-2014.

«Rostelecom» must execute the list of activities of the Russian state program «Information Society (2011 - 2020 years)». This program include the development of the portal of public services, the development of a common space of

trust in electronic signatures, the development of interagency electronic interaction and a single identification system. It is planned that «Rostelecom» will engage the development of mechanisms which enable the use of mobile devices for access to e-government services and to the state-mail address which using for the interaction between citizens and government agencies.

The «Rostelecom» must create the common directories and the qualifiers for the state information systems and it must create the projects such as «Electronic Registry Office», «E-Region» and «E-democracy». The basis for the implementation of these systems is cloud computing platform. The project offers infrastructure and software as a service (IaaS and SaaS).[16]

Strategy of development of branch of information technologies in the Russian Federation for 2014-2020 and on prospect till 2025 provides creation of a national platform of cloud computing.[9] For these purposes the State defines itself as the customer of these works in the Russian market of information technologies.

The «Rostelecom» has developed and has launched cloud platform in August 2011. This platform helps the «Rostelecom» in selling their computing resources and software to third-party. In the future, this platform can be an integrated into the national platform of cloud computing.

Currently, in the Russian Federation plans to create seven powerful data centers, on the basis of which will be provided the cloud services for government agencies and academia. Including, the public services platform «Gospriklad» was developed for the provision of public services. [23]

4. Conclusion

The Decree of the Government of the Russian Federation of July 20, 2011 N 1275 p approved the Concept creation and development of an integrated information system of state management of public finances «Electronic budget». This Concept is recommended to the executive authorities of the Russian Federation and local authorities for the development of systems of public (municipal) finance. The subsystems of the system «Electronic budget» will be available as service subsystems for use by the subjects of the Russian Federation, the municipalities or the government sector organizations on a pro bono basis. The subsystems of the system «Electronic budget» will be submitted as model of «software as a service» (SaaS).

Single portal of the budget system of the Russian Federation will consist of closed and of open parts.

The open part of the portal is being provided as a public information resource, providing free access to the regulatory, statistical and analytical information in the management of public finances.

The storage and the processing is being carried out in a centralized service of the system «Electronic budget» which is a source of information to be placed in the open part of the portal.

Closed part of the portal consists of a «private offices» available to users with the appropriate powers and which have keys of an electronic signature certificates. Closed part of the portal is the single point of user access to the functions of centralized and service subsystems «Electronic budget». This system includes a single, unified system of management of user access levels depending on their powers for the all functions of subsystems «Electronic budget».

The government services will be available to users cloud platform in the areas applications of the medicine, housing, energy, transport and others. In addition, the online service has created for work with documents.

Unfortunately, in the Russian Federation there are not many examples of the use of models of public services based on cloud computing. Although, with 2013 in Russia is being actively implemented the idea of cloud computing in government.

Thus, we need to understand the technology and their reliability before using cloud technology. The ISP of cloud computing should prescribe in the contract the level of service. Of course, the using the cloud computing has disadvantages which carry new risks. These risks are actually as Russia and other country.

Firstly, the user does not own or have not access to the inside the cloud. Safety of the user data is highly dependent from the company's ISP.

Secondly, there are no generally accepted standards in the direction of cloud computing security.

Originally, the owner of the «cloud» developed the standards of the safety. He is free to choose the models and mechanisms of protection.

Thirdly, there is no definite answer about the responsibility of the subject providing the service to the user.

Fourthly, ISP of personal data must ensure conditions of use of electronic signatures.

The results of this study will be used in further science researches that aimed at identifying approaches to organizing and securing the digital economy in Russia.

5. Acknowledgments

We thank the Russian Humanitarian Science Foundation for their assistance in the project “Comparative legal research methods of information security in the Russian Federation and EU Members (№ 16-03-00679)”.

6. References

- [1]. <https://cloudsecurityalliance.org/media/news/csa-survey-reveals-emerging-international-data-privacy-challenges/> (2014) Cloud Security Alliance. Published 2014, 23, September. New Cloud Security Alliance Survey Reveals Emerging International Data Privacy Challenges. Accessed on: 2017-10-13.
- [2]. The Order of the Ministry of Communications and Mass Communications of the Russian Federation N 178 of June 30, 2014 «On the Council of Experts on the use of cloud computing in the Ministry of Communications and Mass Communications of the Russian Federation»
- [3]. The Strategy of the development of the information society in the Russian Federation for the years 2017-2030. approved by the Decree of the President of the Russian Federation of May 9, 2017 No. 203
- [4]. The State Program of the Russian Federation "Information Society (2011-2020)" endorsed by Order of the Government of the Russian Federation No. 1815-r of October 20, 2010
- [5]. Federal law "On Personal Data" No. 152-FZ of July 27, 2006
- [6]. Federal law "On Information, Informational Technologies and Protection of Information" No. 149-FZ of July 27, 2006
- [7]. Federal law "On Electronic Signature" No. 63-FZ of April 6, 2011
- [8]. Federal law "On Communications" No. 126-FZ of July 7, 2003
- [9]. The Strategy of development of branch of information technologies in the Russian Federation for 2014-2020 and on prospect till 2025 endorsed by Order of the Government of the Russian Federation of November 1, 2013. Implementation of the cross-border transfer of personal data
- [10]. The Strategy of the development of the information society in the Russian Federation for the years 2017-2030. approved by the Decree of the President of the Russian Federation of May 9, 2017 No. 203
- [11]. <http://conventions.coe.int/Treaty/EN/Treaties/HTML/108.htm> (1981) The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 28.I. 1981 .Accessed on: 2017-10-13
- [12]. Letter of the Ministry of Communications and Mass Communications of the Russian Federation of 13 May 2009 N CP-P11-2502 «On the implementation of the cross-border transfer of personal data»
- [13]. <http://www.enisa.europa.eu/media/news-items/security-issues-in-cross-border-e-authentication> (2017) Security Issues in Cross-border e-Authentication. Accessed on: 2017-10-13
- [14]. <https://ec.europa.eu/digital-agenda/node/1322> (2017) About Cloud computing. Accessed on: 2017-10-13
- [15]. <http://ieeet.tusur.ru/ru/index.htm> (2016) The Tomsk group and student's office of Institute of engineers on electrical equipment and radio electronics. Accessed on: 2016-11-09
- [16]. http://minsvyaz.ru/ru/monitoring/index.php?id_4=43034 (2017) Official website of the Ministry of Telecom and Mass Communications of the Russian Federation, Accessed on: 2017-12-12
- [17]. Adrian A.. (2013) How much privacy do clouds provide? An Australian perspective, Computer law & Security review, Vol. 29 Issue 1, pp. 48-57 doi.org/10.1016/j.clsr.2012.11.010
- [18]. Baranov A. (2012) Can we protect in the «cloud» of confidential information? .- High availability systems № 2, Vol. 8
- [19]. Zharova A., Elin V. (2017), The use of Big Data: A Russian perspective of personal data security, Computer Law & Security Review, Volume 33, Issue 4, pp. 482-501, doi.org/10.1016/j.clsr.2017.03.025
- [20]. Kanashevsky V.A. (2012) Legal regime of cross-border transfer of Personal Data .- Legislation
- [21]. Noriswadi I. (2011) Cursing the Cloud (or) Controlling the Cloud?. - Computer law & Security review Vol. 27
- [22]. Official site of the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) (Accessed December 12, 2017). Retrieved from: <http://rkn.gov.ru/news/rsoc/news23181.htm>
- [23]. http://minsvyaz.ru/ru/monitoring/index.php?id_4=41944 (2011) In 2011 the Ministry of Telecom and Mass Communications will create a resource - a gospriklad.ru. Accessed on: 2017-12-12
- [24]. The Internet interview to the head of the department of information technologies, communication and information security of the Ministry of Internal Affairs of the Russian Federation, lieutenant general of internal service Tyurkin M. L. «Development and introduction of modern information technologies in system of the Ministry of Internal Affairs of Russia
- [25]. http://minsvyaz.ru/ru/monitoring/index.php?id_4=43034 (2016) Official website of the Ministry of Communications and Mass Communications of the Russian Federation. Accessed on: 2017-10-13
- [26]. <http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment> (2009) Cloud Computing. Benefits, risks and recommendations for information security. November 2009. Accessed on: 2017-10-13.
- [27]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF> (2012) Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions Unleashing the Potential of Cloud Computing in Europe. Brussels, 27.9.2012 . Accessed on: 2017-10-13.
- [28]. Zharova A. K., Elin V. (2015) Legal Aspects of the Use of Educational and Scientific Information Posted on the Internet for Organizing e-Learning According to the Russian Example, in: Strategic Innovative Marketing. 4th IC-SIM, Mykonos, Greece 2015. Switzerland : Springer International Publishing, 2016. doi P. 615-623.

- [29]. Bahtovski A., Gusev M. (2014) Cloudlet Challenges, Procedia of 24th DAAAM International Symposium on Intelligent Manufacturing and Automation, pp. 704–711, doi: 10.1016/j.proeng.2014.03.045
- [30]. Kostoska M.; Gusev M.; Ristov S. (2014) New Cloud Services Portability Platform, Procedia of 24th DAAAM International Symposium on Intelligent Manufacturing and Automation, pp. 1268 – 1275, doi: 10.1016/j.proeng.2014.03.118
- [31]. Katalinic. B.; Kukushkin I.; Pryanichnikov V.; Haskovic D. (2014) Cloud Communication Concept for Bionic Assembly System, Procedia of 24th DAAAM International Symposium, pp.1562 – 1568, doi: 10.1016/j.proeng.2014.03.156
- [32]. Davidovic. V.; Ilijevic D.; Luk V.; Pogarcic I. (2015) Private Cloud Computing and Delegation of Control. Procedia Engineering, Vol.100, pp. 196-205. ISSN: 1877-7058