Issues in Information Systems
Volume 16, Issue IV, pp. 77-85, 2015

THE PRIVACY OF INFORMATION IN CLOUD COMPUTING

Rosarito Sánchez-Morcilio, University of Puerto Rico, Río Piedras Campus, rosarito.sanchez@upr.edu
Francisco Quiles-Torres, University of Puerto Rico, Río Piedras Campus, francisco.quiles@upr.edu

ABSTRACT

This paper presents a literature review about the privacy of information in the cloud computing systems. A simple click after a cloud computing subscription can risk privacy of information. It is advised that the organization develops a cloud computing agreement with the cloud services provider, and with possible third parties. A list of theoretical principles is given to create cloud computing agreements, which must be based primarily on trust. The main contribution of this paper is to exhibit, based on an exhaustive theoretical review, a model for negotiation and agreement between the organization and the cloud computing services provider to comply with privacy of information in the cloud computing environment.

Keywords: Privacy of Information, Data Privacy, Model, Trust, and Agreement

INTRODUCTION

Cloud computing services challenge traditional privacy law concepts as well as regulators who struggle to keep up with technological developments, explained Ritchey, McGregor, & Sendra [34]. Balancing innovation and reasonable protections regarding data privacy and security is currently uncertain and change will be the norm for the years to come.

Technology, more specifically cloud computing, had brought issues that are new to most traditional legal systems. Schwartz [36] study indicated that cloud computing had created a new way in the processing of personal data; these changes had created challenges to existing legal systems. Kalyvas, Overly, & Karlyn [22] explained intellectual property rights are being jeopardized due to the latest advancements in technology. A great example of the challenges that technology present to owner's copyright is the new free application called Periscope, which allow the user to create real time, streamline videos of any event, in potential violation of the rights of the event producers or artists, as pointed out by Menéndez-Sanabria [30]. Due to its success and potential, Twitter decided to purchase Periscope for 400 million US dollars. The author explained that Periscope is not intended for copyright violation and that Twitter administration, upon notification of a potential infringement, removes the content and locks the user account.

The use "bring your own devices (BYOD)" and the availability of mobile applications creates the potential of data loss if the device becomes hacked or lost, which may lead to privacy debates if the device carried third party sensitive information, as Ritchey, McGregor, & Sendra [34] discussed. Mobile applications, according to the California Attorney General, must have clear and conspicuous privacy policies and limited collection of personal identifiable information [34]. European Union asserted mobile applications is subject to its Privacy and Electronic Communications Regulations, which require that users be informed about cookies and consent to their use. A solution offered by the mobile application providers to protect a company's information in a device if it's lost, such as "remote wipes", does protect the company's sensitive information, but also impact any user's personal data, which may lead to potential liability for unauthorized access to the device under state and federal computer trespass laws (Ritchey, McGregor, & Sendra [34]).

Twitter and Facebook focus on social networks with millions of users as Horn-Nord, Paliszkiewicz, & Koohang [20] explained. Twitter, as the authors continued discussing, has a steady grow in popularity due to its tools in support of business social needs, such as people's awareness, marketing, communication and collaboration with customers to build relationships and gain more customers. Another example is Force.com, as Lee, Kim, & Raven [26] established, a platform that stores data in a similar fashion to a relational database. Its user can create objects, similar to

data tables, and use the service to store data in cloud computing services (subsequently referred as the "cloud"). Force.com provides data analytics tools, such as dashboards and reports, in real time. Monitoring key data can lead to success in business. Web 2.0, a media application, is one of the most influential communication media cultivating and building social relationships among employees, customers, and business partners Lee, Kim, & Raven [26]. It is considered the second stage of the World Wide Web (WWW) and supports massive collaborations by dynamic user generated content and growth of social networking, such as Wikipedia, blogging, and social networks.

BACKGROUND

Definitions

The Oxford University Press dictionary [2] defines privacy as the state of being free from public attention. It gives the word peace as a synonym for privacy. Privacy is a fundamental human right [4] [40] and is best recognized in its breach or loss [4]. The Oxford dictionary [1] defines information as data, which are facts produced and stored in a computer. Examples of data are given by Arapinis, Bursuc, & Ryan [5] and Changqing, Yu, Wenming, Yingwei, Yujie, Uchechukwu, & Wenyu [9]. Data includes email classifications, patterns, predefined rules, experiments, observations, as well as mobile device data, sensor data, and streaming data.

Trust management is defined by Grandison & Sloman [14], as "the firm's believe in the competence of an entity to act dependably, securely, and reliably within a specified context". The authors' definition includes many different attributes, which are reliability, dependability, honesty, truthfulness, security, competence, and timeliness. The authors specified that many research scientists had recognized the importance of trust management, but few had defined it. From the technical standpoint, Niu, Reith, & Winsborough [31] defines trust management as a scalable form of access control that relies on delegation.

Privacy of Information

Relevant literature on the privacy of information indicates that the main characteristics are privacy rights, privacy protection, and privacy security. Compliance refers to privacy rights, privacy protection, and privacy security over data pertaining to individuals. Compliance is very challenging to auditors, as Courtney [10], Fernandes, Soares, Gomes, Freire, M. & Inácio [13], and Ward & Sipior [41] explained, because the information may be stored on virtual resources spread across multiple legal jurisdictions at different times.

Privacy Rights

The definition of personal information and automated processes is unclear in most cases, according to Schwartz [36]. The author explained there is no international harmonization of these concepts. Consequently, privacy laws vary internationally. Jurisdiction for legal actions related to cloud computing is an area of concern, especially when data is stored in multiple sites across the world. Cloud service providers with enough resources, as stated by Fernandes, et al. [13], have data center facilities spread all over the world, allowing high data availability and redundancy. Computing activities, such as data storage and application management, can shift rapidly from country to country depending on the load capacity of the systems, as revealed by Schwartz [36].

In the case of a law infringement, determining the jurisdiction where the trial will take place is itself a matter of debate, as discussed by Ward & Sipior [41]. There are cases in which the court cannot assert United States jurisdiction. In the case of international jurisdiction, the determination is more blurred. The authors established customers using cloud computing services could be confronted with litigation under laws which are different from those to which companies are accustomed. The authors discussed the term Internet jurisdiction, which refers to the fact that the Internet had created unusual, non-easy solution legal issues, seldom encountered before in courts.

For cloud computing industry to evolve and grow, while assuring consumer sensitive data protection, King & Raja [25] and Adrian [4], recommended a reform of privacy law. Schwartz [36] advised there is a need for a contract model that would provide protection for business without interfering with the Internet evolution. Legislation for data protection regulations is in evolution, as explained by Courtney [10]. The author advised that a balance between the legal protection of intellectual property and meeting the legitimate need of the organizations is needed.

King & Raja [25] also proposed to protect consumers' information privacy without restricting the cloud computing industry. The price of privacy security should not be the loss of technological innovation, as Adrian [4] highlighted. Legislation for data protection, according to Victor [40], must establish new individual privacy rights to include the right to be forgotten. Unless data can be demonstrated, compelling legitimate grounds for the processing, user data must be erased.

Privacy issues are even more controversial for trade secrets. Dial & Moye [12] defined, according to the Uniform Trade Secret Act, a trade secret to be the kind of information that can derive in economic value and is subject to efforts of maintaining its secrecy. Organizations must, as the authors advised, elaborate contracts in which the employees would never upload trade secret information in public cloud, such as Gmail or Dropbox, not even as a zip file. A private cloud must be provided for this purpose in order to give reasonable protection while encouraging the employee to work from remote locations. If an employee leaves the organization, a robust exit interview protocol must be followed in order to access if critical information had been stored in non-private cloud services. All employees must follow reasonable measures to preserve the confidentiality of trade secrets in the cloud. Also, Dial & Moye [12] recommended the trade secret owners to be proactive when it comes to transfer data into the cloud. Proactive actions are negotiated comprehensively with cloud providers and included in a contractual agreement between the organization and the cloud provider, to determine what information should be excluded from storage it in the cloud, and to obligate employees, from both the organization and the cloud provider, to adhere to well defined cloud use policies, both during the employment and afterwards.

Privacy Protection

Privacy protection is much difficult to enforce when third parties are involved [40]. It is a challenge to implement privacy protection in a big data cloud computing environment [9]. Data is considered to be dynamic because it changes rapidly; it is difficult to protect privacy when data is continuously changing. Privacy protection strategies are mainly focus on static data set, not on dynamic.

Data protection techniques data had been proposed by many authors to facilitate the interaction of two parties who trust each other interchanging information cross border boundaries. Those techniques related to cryptography were presented by Zissis & Lekkas [42] and Arapinis, Bursuc, & Ryan [5]. Data protection is continuously reformed at the European level as well as US legislation, including personal data processed in criminal investigations [6, 34]. In the case of big data, the convenience of an index to manipulate such massive amounts of data and a distributed approach to retrieve results in near real time [9].

Privacy Security

Security concerns have arisen with the increased use of cloud computing services such as Web 2.0 and Internet of Everything (IoE) [13]. It supports massive collaborations by dynamic user generated content and growth of social net working such as Wikipedia, blogging, and social networks. Internet of Everything is new paradigm of the Internet and refers to the ability to connect any device capable of providing web services interfaces by natural human machine interaction [38].

Security in big data consists of how to process data mining without exposing sensitive information of users [9]. Privacy and security issues will continue to develop around the world [34]. Technological advances create opportunities to access and use data in ways that were unimaginable before. But, there are risks associated to those technological advancements. Data risks may affect individuals, companies, and countries. Since data and its applications grow exponentially, it is a challenge to monitor and control data security protection [9]. On-premise cloud services are the alternative for those businesses aware of security issues [13, 42].

Privacy security must be multidimensional, not limited to a firewall or a password [4]. Entities, such as government, businesses, and computers scientists, can leverage the advantages of technology if less focus is on the data location and more attention is on data security [11]. Another alternative is to focus on certifying security practices, developing interoperable cloud hosting platforms, pushing standardizations of contract terms, and ensuring data and workloads are easily portable between clouds [10]. A list of associations, forums, and alliances related to certification and standardization issues in privacy security in cloud computing were provided by Courtney

[10].

Virtual private cloud is what Fernandes, et al. [13] recommends for privacy security. Virtual Private Network (VPN) connectivity delivers a virtual private or semi-private cloud, resulting in isolation of resources to each customer. The authors named Amazon VPC as an example of this kind of cloud.

Cloud Computing Environment

Data analysis, in many cases, is done in the context of cloud computing [9, 28, 19]. Due to cloud computing conveniences, many companies have chosen to process its data in that setting. Findings in the Khanagha, Volberda, Sidhu, & Oshri [24] study indicated cloud computing adoption by business is a gradual and stepwise process aiming to maximal preservation of its data as assets.

Privacy of information is mostly exposed in the cloud computing environment. Schwartz [36] emphasized the privacy issue in cloud computing, which in most cases, involves data management, which includes software, hardware, and company's data, to be performed remotely and in a shared environment. Kalyvas, Overly, & Karlyn [22] argued that in this kind of setting the customer has little or no control over data and its security.

Both groups of authors Kalapatapu & Sarkar [21] and Changqing, et al. [9] had described big data services in cloud computing environment. Database as Service (DaaS) scales out in-memory databases analyzing its data. Examples include Amazon and Force.com. Analysis as Service (AaaS) is an analytic platform on a higher abstraction level of data, which executes scripts and queries that data scientist and programmers develop in order to conduct an in-depth analysis of data. Big data as Service (BDaaS) customizes or create new big data stacks; the user must first acquire the infrastructure and then manually install the big data processing software. For distributed systems, this process can be a challenge.

Trust Management

Trust management is found in different disciplines, such as philosophy, psychology, management, electronic commerce and some others as explained by Paliszkiewicz [33]. Trust management have been related to cloud computing recently, being key for the cloud computing adoption and growth as Saleh, Hamed, & Hashem [35] and Noor, Quan, Zeadalyy, & Jian [32] recalled. Habib, Ries, & Muhlhauser [16] and Habib, Ries, Mühlhäuser, & Varikkattu [17] proposed a multi-faceted Trust Management (TM) system architecture for a cloud computing marketplace. Their system provided a means to identify the trustworthy cloud providers according to different attributes such as information security, performance, data governance, and compliance. Bharathi, Vijayakumar, & Pradeep [8] proposed another Trust Management Scheme for cloud computing, which provides service based on location and real time. Hamoudaand, & Glauert [18] described trust management in cloud computing is more complex than the information owner managing its own computers. There are two parties directly involved in the trust chain: those are the owner's domain and the service provider's platform. The information owner has an inferred trust its data is safe in the provider's platform. The authors mentioned Trusted Computing Group (TCG) is an international computer industry standards organization that specifies and encourages trusting computing techniques. The organization is responsible for keeping updated the Trusted Platform Model (TPM). Its specifications includes a booted environment, ability to store data, identify the user and the system, support security standards and protocols, support multiple users on the same system while preserving security and produce an inexpensive system. Hamoudaand, & Glauert [18] recommended to focus first in securing the data and then on securing the infrastructure. Abbadi [3] proposed a self-managed system to test trust for cloud services. Becker [7] presented a framework on security protection when cloud services are in use.

Main Contribution of the Paper

This paper presents a model for negotiation and agreement between the organization and the cloud computing service provider for complying with privacy of information in the cloud computing environment. The model was developed on trust management from the management standpoint, as described by Paliszkiewicz [33].

Organizations such as lawyers, medical doctors, insurance companies, banks, engineering and government manage highly confidential data. Arapinis, Bursuc, & Ryan [5] explained those organizations are skeptical of using cloud computing services because of the confidentiality and security risk that may be associate to those services.

The main contribution of the paper is to show a model for negotiation and agreement between the organization and cloud computing service providers to comply with privacy of information within the cloud computing environment. The model is called the Eight Concepts Cloud Computing Privacy Model, created based on Paliszkiewicz [33] trust management theory, which could facilitate negotiation and agreement between the organization and the cloud computing service provider in the best interest of the customers' information privacy in the cloud computing environment.

METHODOLOGY

This paper is theoretical in nature. The model for negotiation and agreement between the organization and the cloud computing provider is developed according to following principles:

1. In cloud computing environment, the organization trust a third party to manage its data resources. Cloud computing brings significant cost savings, instantaneous data access and reliable data storage according to Dial & Moye [12] Cloud computing disadvantages includes the potential loss of valuable information. In the event of data damage, the responsibility relies on the data owner (the organization), rather than the cloud service provider. The organization's customer is directly affected, since his or her data may be exposed in a data damage situation.
2. The allocation of privacy roles in the cloud computing environment, as Balboni & Pelino [6] explained, raises complex and challenging questions regarding regulations and legislation.
3. Security and privacy issues are solved when essential trust is maintained [42].
4. Partnering with the cloud service provider and establishing a governance structure for cloud computing are very important steps towards transparency in data management [41].
5. Since the legal systems do not contemplate all the technological issues that involve cloud computing, it relies heavily on contracts between entities [36, 13].
6. The organization is responsible for its customer's data. Data trust relies mostly on the organization. Organizations are expected to protect its customers' data. For that reason, it is advised organizations to have insurance, as most data privacy and security laws hold them liable for a security breach, no matter if it is the organization's or the cloud provider's fault [22]. A cyber-liability policy is available to protect the organization against data security issues. It is recommended that both the organization and the provider hold insurance policies.
7. Jurisdiction and territoriality related to privacy regulation is the key area of an ongoing cloud debate. Ritchey, McGregor, & Sendra [34] explained there are generally two bases for jurisdiction over the cloud: the location of the infrastructure (servers or data centers) and the location of the provider.
8. Data as a commodity must be limited to the consumer's right to fully sell her personal information on the open market [36].

FINDINGS

Literature review suggests a model for negotiation and agreement between the organization and the cloud computing service provider, with assurance of privacy of information within the cloud computing environment. The model is shown in Figure 1. Since the model involves eight important concepts, the model is called the Eight Concepts Cloud Computing Privacy Model.

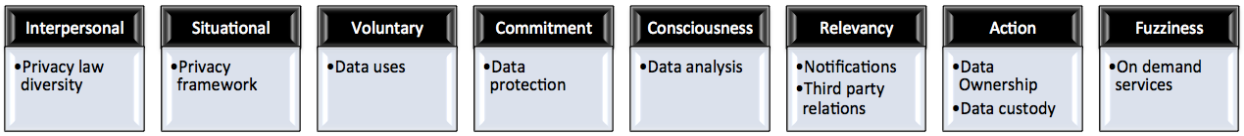

Figure 1. The Eight Concepts Cloud Computing Privacy Model: Model for Negotiation and Agreement Between the Organization and the Cloud Computing Service Provider for Complying with Privacy of Information in the Cloud Computing Environment

The model illustrated in the figure was created based on the trust management theory from Paliszkiewicz [33]. Trust

management characteristics are, as the author describes, interpersonal, situational, voluntary, commitment, consciousness, relevancy, action, and fuzziness. Each trust management characteristic has an agreement strategy related to it. The agreement recommendations are taken from Gilbert [15], Kalyvas, Overly, & Karlyn [22], Kalyvas, Overly, & Karlyn [23], King & Raja [25], Ritchey, McGregor, & Sendra [34], Schwartz [36], and Zissis & Lekkas [42].

Interpersonal is the first characteristic described by Paliszkiewicz [33] and requires both parties to be involved in the negotiation, communicating openly and transparently. This implies the agreement must clearly establish, as Schwartz [36] recommended, the privacy laws of the country or countries involved, making sure both parties understand its implications. The privacy of information includes not only the organizational customers' data, but also the automated processes that need to be performed in order to manage that data. On demand access to the network, as Mell & Grance [29] explained, allows the organization to use a variety of resources of hardware and software, with minimum interaction with the service provider. Even so, it is advised to have a contract before starting any network relationship. For example, Amazon Elastic Compute Cloud (EC2) allows using powerful infrastructure for simulations at a very low cost per user [37]. It is advised to settle a contract before managing the organizational data in a server whose provider is not related directly to the responsibilities for privacy of information through a contract.

Situational is the second characteristic. It implies parties must be clear, consistent, and predictable about the responsibilities of each other to guarantee privacy of information for the sake of the consumer, whose data is managed (Paliszkiewicz [33]). This indicates the agreement must include the list of locations data is being stored and the privacy laws in each jurisdiction present when multiple locations are involved. The contract must present a legal framework that ensures appropriate privacy and confidentiality protection [42].

Voluntary is the third characteristic and is related to the willingness of both parties to comply with privacy of information for the best interest of the consumer, whose data is involved [33]. This advocates for the agreement to include the willingness of the service provider of not using the client's data in any form, except when manipulated to provide the required service [22].

Commitment is the fourth characteristic refers the loyalty that must exist among the parties involved, who must act from the benefit of each other [33]. This characteristic suggests that a contract or agreement between both parties is essential to clarify how data will be managed in the best interests of the organization, while aiming to protect its privacy (Gilbert [15]). The most important aspect regarding data protection regulations is the transparency in data management from the cloud service providers to its clients [6]. The aim is to protect the fundamental rights of the individuals as per the United Nations Universal Declaration of Human Rights (UDHR).

Consciousness is the fifth characteristic relates to the awareness both parties need to have to fulfill each other business [33]. The service provider must commit to not share the client's data in anyway, not even by removing its identifiers, without the client's consent (Schwartz [36]). Another clause in the contract must be to establish the cost of other activities that may be required in the future. In fact, it is advised to run a test, previously agreed upon, of the importing and exporting of data before entering in a formal relationship with the provider [22].

Relevancy is the sixth characteristic and denotes the consequences of the trust breaching [33]. The organization has delegated data control to the cloud services provider, but from legal standpoint, the organization maintains the privacy of its information. The agreement must include a statement where the cloud service provider shares responsibility for data breaching. Even though regulations in the USA and EU are different, a common is that they both have an agreement to notify any data breach that may occur [34]. The agreement must specify that a notification to all parties involved must proceed in the case of data breaching. Moreover, there must be contractual protection to information security, and joint liability [22]. It is also important to consider the location of the data centers where the data is physically stored and who may manage the data. The organization needs to be aware of the location of the data center because privacy laws vary among different jurisdictions [25]. In the case a third party may be managing some of all the data of the organization, it is recommended that the organization should start a contractual relationship with that third party as well [22].

Action is the seventh characteristic and indicates that both parties must have a common goal of striving for privacy of information excellence [33]. Both parties must clarify and explore specific expectations from each other, as the common goal must be to protect consumers' data. The organization should know where its data may be located at all times [42]. This may represent a challenge in the cloud computing environment. The actions to be established in the contract vary according to the involved countries. The European Union and United States are the major players in cloud computing [25]. These countries' data privacy protection framework is described by Ritchey, McGregor, & Sendra [34]. The authors also provided the privacy protection framework for Philippines, South Korea, Australia, Peru, Costa Rica, and Colombia.

Fuzziness is the eighth characteristic and points out that it is impossible to predict if both parties can trust each other in the long run [33]. Only after a period of time, it can be certain if, indeed, one party can trust the other. As fuzziness in trust may exist, the agreement must have a beginning and an ending date of validity. The agreement can be renewed again according to previous experiences. Fuzziness yields that the agreement indicates the delivery of the software and hardware over the Internet, scalability on-demand (use as needed), and its payment is based on the customer's actual use over a period of time [22]. In addition, the contract or agreement between both parties should state how the privacy of the data will be managed to the best interest of the organization. The organization hiring cloud computing services is the only one responsible for the adequate security, data protection, and backups [15]. The cloud computing service provider may retain the unilateral right to change the terms, including price, or suspend or terminate the services at any time or on short notice, or to process data in any country in which it does business. The organization is responsible for legal compliance with the applicable data protection laws no matter where the service provider stores its data, even if the service provider has not notified the organization of where it has store its data.

In summary, the agreement between the organization and the cloud computing provider is founded on trust management and must show the belief and its facts that relations will be successful.

DISCUSSION

Recommendations

The model is recommended to organizations holding and managing sensible data. In order to maximize privacy of data, organizations must follow the model before participating in the cloud environment. Once the negotiations and agreements are established, a trust management system, from the technical standpoint, can be adopted to successfully operate in a cloud computing environment.

Negotiation and Agreement

The cloud computing atmosphere involves three parties: the organization (the company that utilizes the service), the cloud computing provider (service provider), and the customer (who receives services from the organization and whose data must be private and protected). The model is proposed to be used as guidance for the negotiation and the agreement between the organization and the cloud computing provider in the best interest of the customers' information privacy in the cloud computing environment.

CONCLUSIONS

The major characteristics in privacy of information, which are privacy rights, privacy protection, and privacy security, were discussed. A description of the cloud computing was presented as well. Since the organization is primary responsible for privacy of information, it need to establish a trustful relation with its cloud computing service provider. It is paradoxical that recommendations for technology issues can be found outside its theory. The model presented in the article, called the Eight Concepts Cloud Computing Privacy Model, can be used as a reference when elaborating a contract between a cloud service provider and a client. The main characteristic of the agreement should be that it must be based on trust. To comply with privacy of information, both the organization and the cloud computing service provider, must work towards the best interests of the consumer and always aim for a common good. Since the model was constructed on theory, future work can be focused on surveying senior executives to learn about their experiences with cloud computing services and contract agreements. Due to the relevance of information privacy in cloud computing, Ling, Yang, Gallagher, Pailthorpe, Sadiq, Heng Tao, & Xue [27] and Topi,

Valacich, Wright, Kaiser, Nunamaker Jr, Sipior, & De Vreeda [39] agreed that academia must address that topic in curricula. Changqing, et al. [9] recommended that academia and industry collectively study the great opportunities in data analysis, while complying with the privacy laws of the different countries for the long term success of evolution for cloud computing.

REFERENCES

1. "information, n." *OED Online*. Oxford University Press, March 2015. Web. 2 May 2015.
2. "privacy, n." *OED Online*. Oxford University Press, March 2015. Web. 2 May 2015.
3. Abbadi, I. (2013). A framework for establishing trust in Cloud provenance. *International Journal Of Information Security, 12*(2), 111-128. doi:10.1007/s10207-012-0179-0
4. Adrian, A. (2013). How much privacy do clouds provide? An Australian perspective. *Computer Law & Security Review 29*(2013), 48-57.
5. Arapinis, M., Bursuc, S., & Ryan, M. (2013). Privacy-supporting cloud computing by in-browser key translation. *Journal Of Computer Security, 21*(6), 847-880. doi:10.3233/JCS-130489.
6. Balboni, P., & Pelino, E. (2013). Law Enforcement Agencies' activities in the cloud environment: a European legal perspective. *Information & Communications Technology Law, 22*(2), 165-190. doi:10.1080/13600834.2013.821812
7. Becker, M. Y. (2012). Information flow in trust management systems. *Journal Of Computer Security, 20*(6), 677-708.
8. Bharathi, C., Vijayakumar, V., & Pradeep, K. (2015). An Extended Trust Management Scheme for Location Based Real-time Service Composition in Secure Cloud Computing. Procedia Computer Science, 50(1), 103-108.
9. Changqing, J., Yu, L., Wenming, Q., Yingwei, J., Yujie, X., Uchechukwu, A., & Wenyu, Q. (2012). Big data processing: Big challenges and opportunities. *Journal Of Interconnection Networks, 13*(3/4), 1-19. doi:10.1142/S0219265912500090
10. Courtney, M. (2013). Regulating the cloud crowd. *Engineering & Technology, 8*(4), 60-63.
11. Desai, D. (2013). Beyond Location: Data Security in the 21st Century. *Communications Of The ACM, 56*(1), 34-36. doi:10.1145/2398356.2398368
12. Dial, A. A., & Moye, J. M. (2014). Trade secrets in the cloud: Assessing and mitigating the risks. *Journal Of Internet Law, 17*(11), 1-23.
13. Fernandes, D., Soares, L., Gomes, J., Freire, M., & Inácio, P. (2014). Security issues in cloud environments: A survey. *International Journal Of Information Security,13*(2), 113-170. doi:10.1007/s10207-013-0208-7
14. Grandison, T. S. (2000). A survey of trust in internet applications. *IEEE Communications Surveys & Tutorials*, 3(4), 2-16.
15. Gilbert, F. (2011). Cloud Service Providers as Joint-Data Controllers. *Journal Of Internet Law, 15*(2), 3-13.
16. Habib, S.M.; Ries, S.; Muhlhauser, M. (2011). "Towards a Trust Management System for Cloud Computing," *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on*, vol., no., pp.933,939, 16-18 Nov. 2011
17. Habib, S. M., Ries, S., Mühlhäuser, M., & Varikkattu, P. (2014). Towards a trust management system for cloud computing marketplaces: using CAIQ as a trust information source. *Security And Communication Networks*, 7(11), 2185-2200.
18. Hamoudaand, S. K., & Glauert, J. (2011). *Security, Privacy, and Trust Management, Issues for Cloud Computing*. (B. Benathallah, Ed.) CRC Press.
19. Hashem, I. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Ullah Khan, S. (2015). The rise of "big data" on cloud computing: Review and open research issues. Information Systems, 47(1), 98-115.
20. Horn-Nord, J., Paliszkiewicz, J., & Koohang, A. (2014). Using social technologies for competitive advantage: Impact on organizations and higher education. *Journal Of Computer Information Systems*, 55(1), 92-104.
21. Kalapatapu, A., & Sarkar, M. (2011). Cloud Computing. In B. Benatallah (Ed.), Cloud Computing: Methology, Systems, and Applications (pp. 3-29). CRC Press.
22. Kalyvas, J. R., Overly, M. R., & Karlyn, M. A. (2013:II). Cloud Computing: A Practical Framework for Managing Cloud Computing Risk--Part II. *Intellectual Property & Technology Law Journal, 25*(4), 19-27.
23. Kalyvas, J. R., Overly, M. R., & Karlyn, M. A. (2013). Cloud Computing: A Practical Framework for Managing Cloud Computing Risk--Part I. *Intellectual Property & Technology Law Journal, 25*(3), 7-18.
24. Khanagha, S., Volberda, H., Sidhu, J., & Oshri, I. (2013). Management Innovation and Adoption of Emerging

Technologies: The Case of Cloud Computing. *European Management Review, 10*(1), 51-67. doi:10.1111/emre.12004
25. King, N. J., & Raja, V. (2013). What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data. American Business Law Journal, 50(2), 413-482. doi:10.1111/ablj.12012
26. Lee, J., Kim, B., & Raven, P. (2014). Cloud Computing: Enterprise 2.0. *Issues in Information Systems, 15*(2), 110-115.
27. Ling, C., Yang, L., Gallagher, M., Pailthorpe, B., Sadiq, S., Heng Tao, S., & Xue, L. (2012). Introducing Cloud Computing Topics in Curricula. *Journal Of Information Systems Education, 23*(3), 315-324.
28. Marković, D. S., Branović, I., & Popović, R. (2014). Review of Cloud Computing in Business. Singidunum Journal Of Applied Sciences, 673-677. doi:10.15308/SInteZa-2014-673-677.
29. Mell, P., & Grance, T. (2011). The National Institute of Standards and Technology definition of cloud computing. United States Department of Commerce, *Special Publication* 800-145, available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
30. Menéndez-Sanabria, P. (2015, 5, 9). Periscope revoluciona la transmission de eventos en línea. El Nuevo Día.
31. Niu, J., Reith, M., & Winsborough, W. H. (2014). Formal verification of security properties in trust management policy. *Journal Of Computer Security, 22*(1), 69-153. doi:10.3233/JCS-130490
32. Noor, T. H., Quan, Z. S., Zeadally, S., & Jian, Y. (2013). Trust Management of Services in Cloud Environments: Obstacles and Solutions. *ACM Computing Surveys, 46*(1), 12-12:30. doi:10.1145/2522968.2522980
33. Paliszkiewicz, J. O. (2011). Trust Management: Literature Review. Management (18544223), 6(4), 315-331.
34. Ritchey, K., Paez, M., McGregor, V., & Sendra, M. (2013). Global Privacy and Data Security Developments--2013. *Business Lawyer, 69*(1), 245-254.
35. Saleh, A.S.A.; Hamed, E.M.R.; Hashem, M., "Building trust management model for cloud computing," *Informatics and Systems (INFOS), 2014 9th International Conference on*, vol., no., pp. PDC-116,PDC-125, 15-17 Dec. 2014
36. Schwartz, P. M. (2013). Information privacy in the cloud. University Of *Pennsylvania Law Review, 161*(6), 1623-1662.
37. Srivastava, K., & Kumar, A. (2011). A New Approach of CLOUD: Computing Infrastructure on Demand. *Trends In Information Management, 7*(2), 145-153.
38. Suciu, G., Halunga, S., Apostu, A., Vulpe, A., & Todoran, G. (2013). Cloud Computing as Evolution of Distributed Computing - A Case Study for SlapOS Distributed Cloud Computing Platform. *Informatica Economica, 17*(4), 109-122. doi:10.12948/issn14531305/17.4.2013.10
39. Topi, H., Valacich, J. S., Wright, R. T., Kaiser, K., Nunamaker Jr, J. F., Sipior, J. C., & De Vreeda, G.-J. (2010). IS 2010: Curriculum Guidelines for Undergraduate Degree Programs in Information Systems. *Communications of AIS 2010* (26), 359-428.
40. Victor, J. M. (2013). The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy. *Yale Law Journal, 123*(2), 513-528.
41. Ward, B. T., & Sipior, J. C. (2010). The Internet Jurisdiction Risk of Cloud Computing. *Information Systems Management, 27*(4), 334-339. doi:10.1080/10580530.2010.514248
42. Zissis, D. & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28*(2012), 583-592.