Journal of
Mass Communication & Journalism

Kalloniatis, J Mass Communicat Journalism 2016, 6:3
DOI: 10.4172/2165-7912.1000306

Research Article Open Access

Increasing Internet Users Trust in the Cloud Computing Era: The Role of Privacy

Christos Kalloniatis*

Department of Cultural Technology and Communication, University of the Aegean, Greece

Abstract

During the last decades Internet has been introduced in our lives providing a vast amount of e-services in various fields of our every day activity like banking, shopping, entertainment, communication, learning an so on that without doubt improve our life's quality in various ways. The easiness of use along with the continuously increased number of users joining the online world every day has transformed the use of online services a mandatory daily activity rather than an optional interaction like it used to be in its the early stages. This tremendous development inspired many professionals and IT experts to invest in the creation of more innovative web services that will increasingly attract more users offering even more attractive ways to improve the quality of living both in the physical/real and online worlds. One of these recent innovations is the creation of cloud computing, a three layer architecture that offers various kinds of services that users enjoy. Users' trust towards cloud computing is one of the greatest socio-technical issues today and one of the key factors that formulate users' trust is the protection of their privacy. This paper moves towards this direction identifying the privacy characteristics that must be realized when designing services for cloud users.

Keywords: Internet trust; Security; Privacy; Cloud computing; World wide web

Introduction

A major challenge in today's online world is to make users trust the software they use in their everyday professional or recreational activities. Trusting software depends on various elements, one of which is the protection of users' privacy. Protecting privacy is about complying with users' desires when it comes to handling personal information. It can also be defined as the right to determine when, how and to what extend information about them is communicated to others.

During the last decade, privacy has gained great attention especially from online Internet users participating in incidents regarding unauthorized data exploration, misuse of information stored in social media websites, data undetectability over the Internet, disclose of personal information to third parties without users' consent or without their willingness. Based on two researches conducted [1,2] in 2014 concerning Internet users' feelings regarding their privacy when they are online, 92% of them answered that are afraid about the available amount of their personal data existing online without their consent. In the same research, 58% of users asked are afraid that their personal data are given to third parties without their approval, while 47% believe that their actions are monitored while online in order to get targeted advertisements and web content. Also, 59% of users asked believe that they cannot be anonymous online while the same percent of users believe that they should be able to be anonymous in cases where identification is not required for accessing a resource or service. Finally some 68% of Internet users believe that current laws are not good enough in protecting people's privacy online, while 24% believe that current laws provide reasonable protections. Thus, it is obvious that privacy needs to be considered when realizing information systems or independent services irrespective of the functional environment the system or services will be demonstrated.

The introduction of cloud computing has introduced various new ways for satisfying users' desires online. Scalable storage capabilities, more on-demand services, new innovative platforms and end services directly offered to users are just few of the characteristics that attracted Internet users in adopting it. Although privacy is common concern in distributed information systems, additional privacy issues arise due to the nature of cloud computing. The main advantages of cloud computing namely its ability to scale rapidly, to store data remotely and to share services in a dynamic environment have also created a number of vulnerabilities in terms of data protection. These vulnerabilities are reflected in a number of security threats reported [3-5]. We have compiled a comprehensive list of 14 cloud related threats and vulnerabilities indicating the cloud service model, to which they apply [6]. All of the identified threats and vulnerabilities represent potential circumstances that may lead to misuse of information or resources. However, in order to deal with these circumstances, it is important to identify the privacy-related properties that are affected by each threat or vulnerability. The concepts presented here besides the previous works already stated are also identified based on the European Commission Draft Report on Security Issues in Cloud Computing [7,8] as well that on the report on privacy issues in the cloud era [9]. This paper aims at revealing the key privacy factors that play an important role in raising Internet users' trustworthiness towards the adoption of cloud-based services. Section 2 presents the trust factors both from a technical and social perspective. Section 3 presents the basic characteristics of the cloud computing environments. Section 4 introduces a set of privacy concepts that upon realization can assist in elevating Internet users' trust on the services offered from the cloud service providers. Also it provides a matching of these concepts with the responsible parties, either simple users or cloud providers that should be committed for their implementation. Finally, section 5 concludes the paper by raising issues for future research.

***Corresponding author:** Kalloniatis C, Department of Cultural Technology and Communication, University of the Aegean, University Hill, Mytilene, Lesvos Island, Greece, Tel: +30 2251036637; Fax: +30 22510 29157; E-mail: chkallon@aegean.gr

Received June 24, 2016; **Accepted** June 28, 2016; **Published** June 30, 2016

Citation: Kalloniatis C (2016) Increasing Internet Users Trust in the Cloud Computing Era: The Role of Privacy. J Mass Communicat Journalism 6: 306. doi:10.4172/2165-7912.1000306

Trust factors

Trusting online context was not a first priority for the majority of online users during the past where the willingness to take advantage of a web service and the benefits out of it was the primary and ultimate goal for them. However, as time progressed, users' awareness about Internet increased parallel to the growth of available providers offering the same services. Thus, Internet users, with greater awareness, IT skills and variety of options to choose from, are more demanding when it comes to select the most appropriate service. One key factor is users' trust when selecting a service.

Online trust has many similarities but also differences from offline (physical trust). Unlike offline trust, online trust depends on the Internet and associated technologies. Technological determinants of online trust may include security features, privacy protection mechanisms, aspects of the interface design (ease of use) and system reliability. Nevertheless, social trust factors reflecting users' past experience and perceived trustworthiness of the organization behind the website are still associated with website trust [10,11]. Digital trust in general focuses on the trust relationships between multiple autonomous agents in networked environments [12,13]. Research has also shown that online trust mediates the relationship between website characteristics and user's intentions [14]. In other words, a website or a webservice is 'trusted' because it meets the needs of the users communities for which they are designed [15].

In our previous work [16] we have proposed a trust model that explores the connection between users needs and trust, aiming to define the different trust issues affecting the achievement of users goals. The paper presented a trust model regarding the use of museum websites. It entailed the assumption that approaching trust exclusively from a technical/specifications perspective does not ensure an adequate understanding of a multi-faceted construct. It is argued that technology alone cannot adequately explain audience preferences related to on-line behaviors. Thereby, technological specifications approaches in conjunction with social/behavioral data allowed to understand on-line behavior as primarily human behavior. The model proposed is presented in Figure 1. This model builds upon the 'hard trust' and 'soft trust' approach proposed [17]. "Hard" trust builds upon technical system specifications based on objective regulations and standards. "Soft" trust considers trust based on users' subjective perceptions relating to their online expertise or to the organization supporting the system.

As it can be seen from the aforementioned model, technical issues play an important role in ensuring users' trust. Of course the majority of Internet users are not highly IT skilled professionals able to understand how each security or privacy technology works. This is why technologically enforced trust can be expressed in various forms. Specifically, a number of hard/technical trust parameters relate to the website security and privacy protection. Most system users (especially users that depend upon online systems to take advantage of specific services) feel more convenient when they are provided with assurances that the personal data they provide for the realization of a specific transaction are protected. Even the existence of a privacy policy usually appeases online users even though no evidence of specific types of usage is provided. Security deals with the integrity and confidentiality of data. Implementing security mechanisms for the users and data protection is of vital importance when a museum tries to build trust. The availability of the website is another important trust factor. Eligible users should always have access to e-services based on their access rights. Unjustified denial of service to eligible users lowers their trust. Reliability is also a key issue, as repeated visitation is related to satisfied users' requests. Furthermore, usability is related to trust as users favor easy- to- use, thus easily accessible websites [15,18,19]. In this paper we identify and present the cloud concepts that purely assist on the elevation of trust through privacy implementation.

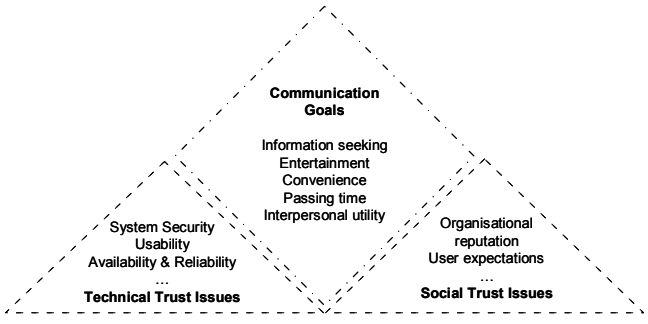

Figure 1: Trust model regarding the use of museum websites [Kavakli].

Cloud computing

Cloud computing is the delivery of computing and storage capacity as a service [12] to a community of end-recipients. Cloud computing entrusts services with a user's data, software and computation over a network, following a logical diagram as shown in Figure 2. Cloud computing providers known as Cloud Service Providers (CSPs) offer their services according to three fundamental models [20-22]: a) Infrastructure as a Service (IaaS), where users rent use of servers provided by one or more cloud providers; b) Platform as a Service (PaaS), where users rent use of servers and the system software to use in them; and c) Software as a Service (SaaS), where users rent both application software and databases. In the cloud, IaaS is the most basic and each higher model abstracts from the details of the lower models as it is graphically shown in Figure 3.

Cloud computing provides the following characteristics:

a. Agility, which improves users' ability to re-provision technological infrastructure resources.

b. Cost, which is reduced since infrastructure is typically provided by a third party and does not need to be purchased for one-

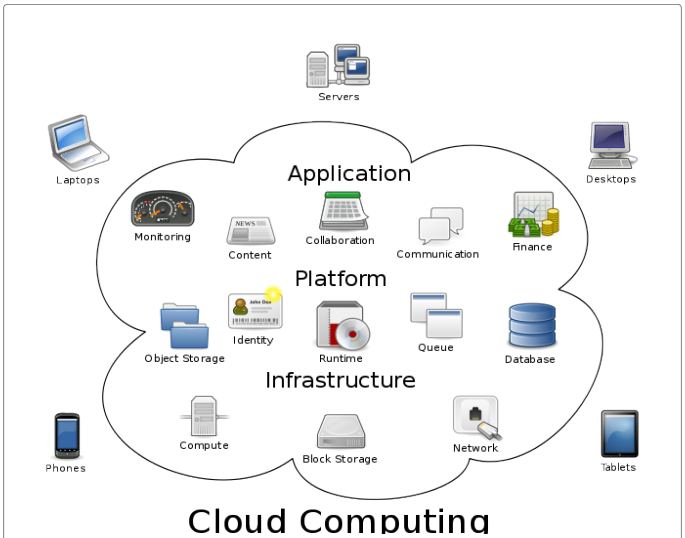

Figure 2: Cloud computing logical diagram.

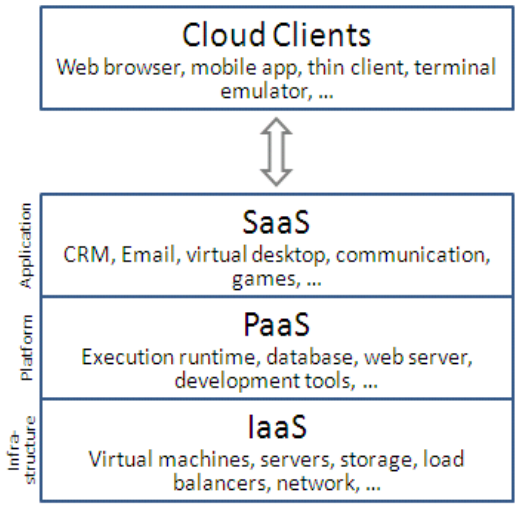

Figure 3: Cloud computing layers.

time or infrequent intensive computing tasks. Also the cost of IT skills is lowered since in-house implementation is avoided [23].

c. Virtualisation, which is the basic technology used in cloud environments allowing servers and storage devices to be shared thus increasing utilization. Applications are usually being migrated from one server to another depending on the capacity and usage of the cloud providers' infrastructure.

d. Multitenancy, which enables the sharing of resources and cost across a large pool of users allowing centralization of infrastructure, increment of peak-load capacity and systems' utilization and efficiency improvement [24].

e. Reliability, which is improved if multiple redundant sites are used and which makes well-designed cloud computing suitable for business continuity and disaster recovery [25].

f. Scalability and elasticity, which support the on-demand provisioning of resources on a fine-grained self-service basis near real-time without users having to engineer for peak loads [26,27].

g. Device and location independence, which support users to access cloud services from anyplace through a web-browser regardless of the device they are using or the location they are accessing the service from [28].

h. Maintenance, which is easier since there is no software installation on each user's machine and the services' sources are managed and updated from a single third party.

It is worth mentioning, that although the combination of the above characteristics is what provides the various advantages of cloud computing, it is the same combination that introduces new security and privacy challenges and requires different solutions.

Privacy in the Cloud

The need for raising Internet users' trustworthiness as presented before is indeed one of the most challenging issues in the online world. Raising trust through privacy in complex, distributed environments like cloud computing is not an easy task. This section moves towards this direction by identifying and presenting the privacy aspects that all respective social and technical actors involved in the systems' development phase should consider.

Isolation

The specific concept refers to the complete seal of user's data inside the cloud computing environment. Isolation is meant to address data disclosure in two ways. Firstly, from purpose limitation point of view and secondly from the aspect of the proper technical implementation techniques [7]. Cloud computing resources are shared among a multitenant environment. Thus, excessive cloud employee's access rights, pose the risk of any kind of Personal Identifiable Information disclosure which may lead to client's privacy violation. The specific concept is matched with the following threats derived from [4], Abuse and Nefarious Use of Cloud Computing, Insecure interfaces and APIs, Malicious Insiders, Shared technology issues, Data Loss or Leakage, Privileged user access and Lack of Data Segregation.

Provenanceability

The specific concept refers to the provenance of the data related to the authenticity or identification, the quality of the results of certain procedures, modifications, updates and vulnerabilities, the provenance of certain actions inside the cloud, the detection of origins of security violations of an entity [29], the auditability of client's data and matters that are related to the cloud's subsystem geographical dispersion in reference to the legal issues, regulations, policies and each country's rules as far as data processing and protection is concerned. All the above constitute a potential privacy violation if they are not realised properly by implementing the appropriate technical measures.

Traceabillity

Traceability concept aims to give the user the ability to trace his/her data or not. This property is examined from the proper/improper data erasure aspect, which is a major problem in web-based systems and still continues to exist in clouds. Many cases have been documented for privacy violation due to improper data deletion (documents, photos, etc.). The traceability concept aims to protect privacy, through the ability of tracing them among the data repositories and reassuring that the data have been completely deleted or maintained invisible and anonymized after their deletion. The clients should be able to trace the physical location of their data and to be able to verify that they are processed according to their collection purpose.

Intervenability

Intervenability concept refers to the fact that the users should be able to have access and process of their data despite the cloud's service architecture. A cloud vendor may rely on other provider's subcontractor services in order to offer him/her services. That should not be an obstacle for the user to intervene with his/her data in case he/she suspects that his/her privacy is violated by the subcontractors. In fact cloud vendor must be able to provide all the technical, organizational and contractual means for accomplishing this functionality for the user including all respective subcontractors that the vendor cooperates and interrelates [7]. The same applies for the situation that a cloud vendor or the subcontractors are bankrupted and client's data are moved to another provider.

CSA accountability

Accountability concept refers to the fact that cloud providers should be able to provide at any time information about their data protection policies and procedures or specific cloud incidents related to users'

data. The cloud architecture makes a complex form of an information system. In terms of management and audit controls, this fact could result in very difficult manageability of the protections mechanisms and incidents. In case of a privacy violation, a cloud provider should be able to provide information about what, when and how an entity acted and which procedures were followed to tackle it [7].

Anonymity

The property anonymity means the state of being anonymous or virtually invisible, having in this way the ability to operate online without being tracked [30]. Therefore, anonymity is the ability of a user to use a resource or service without disclosing his/her identity [31]. Anonymity serves the great purpose of hiding personal identifiable information when there is no need of revealing them. Browsing the Internet only for collecting information is one of many issues that anonymity plays a significant role and must be attained.

Pseudonymity

Pseudonymity is the user's ability to use a resource or service by acting under one or many pseudonyms, thus hiding his/her real identity. However, under certain circumstances the possibility of translating pseudonyms to real identities exists. Pseudonyms are aliases for a user's real identity. Users are allowed to operate under different aliases. Nevertheless revelation of user's real identity occurs when acting unlawfully. Pseudonymity has characteristics similar to anonymity in that user is not identifiable but can be tracked through the aliases he/she uses [30]. Pseudonymity is used for protecting user's identity in cases where anonymity cannot be provided (e.g. if the user has to be held accountable for his/her activities [31,32]).

Unlinkability

The property unlinkability expresses the inability to link related information [30]. In particular, unlinkability is successfully achieved when an attacker is unable to link specific information with the user that processes that information. Also unlinkability can be successfully achieved between a sender and a recipient. In this case unlinkability means that though the sender and recipient can both be identified as participating in some communication, they cannot be identified as communicating with each other. The ability to link transactions could give a stalker an idea of one's daily habits or an insurance company an idea of how much alcohol a family consumes over a month. Ensuring unlinkability is vital for protecting user's privacy.

Undetectability and unobservability

The property of undetectability expresses the inability to detect if a user uses a resource or service. A. Pfitzmann defines undetectabilty as the inability of the attacker to sufficiently distinguish if an item of interest exists or not [32]. In his previous works undetectability was absent as a privacy concept and the gap was fulfilled by unobesrvability. However, since 2010 undetectability is used as the concept for defining the inability of data, processes or user detection from an attacker's perspective. Undetectability is usually used to satisfy steganographic systems where information hiding plays a crucial role.

Undetectability has nothing to do with anonymity- it does not mention any relationship between item of interest and subjects. Even more, for subjects being involved in an IOI, undetectability of this item of interest is clearly impossible. As Pfitzman states, early papers designing new mechanisms for undetectability designed the mechanisms in a way that if a subject necessarily could detect an item of interest, the other subject(s) involved in that item of interest enjoyed anonymity at least [32]. Thus, unobservability is defined as the undetectability that uninvolved subjects have in a communication together with anonymity even if items of interest can necessarily be detected by the involved subjects.

Privacy Property	Internet User	Cloud Service Provider
Isolation	Low	High
Provenanceability	Low	High
Traceability	Medium	High
Intervenability	Medium	High
CSA Accountability	Low	High
Anonymity	High	Medium
Pseudonymity	High	Low
Unlinkability	Medium	High
Undetectability	Medium	High
Unobservability	Medium	High

Table 1: Level of interference per privacy property.

In the Table 1 above the level of interference on the realization of every privacy concept regarding the roles involved is presented. A three-scale categorization is used for expressing the degree of control from every actor, namely low, medium and high. Thus for isolation the cloud service provider has the greater responsibility to address this issue while the user has low. In Anonymity though things change. Preserving anonymity has to do with the users' awareness on security issues, personal data handling, safe behavior while online etc. The CSP will provide the necessary infrastructure but cannot satisfy users' anonymity online if the user is not aware in the sense discussed before.

Conclusion

Cloud computing is one of the most modern, innovative and complex technological environments of the twenty first century leading on its adoption by more and more services offered online today especially due to the innovative characteristics and the scales of economy that it offers. However, nowadays, the more demanding and IT aware modern Internet users feel that trusting the system or service they use is very important in order to proceed with its use. System trustworthiness is a complex, multidimensional sociotechnical factor that needs to be examined in various layers and depths.

This paper is an initial step towards this direction. Specifically, in this paper, privacy as one of the technical dimensions of trust was examined in the context of cloud computing. Specifically the concepts that need to be taken into consideration both by the users and the service providers when designing privacy-aware cloud-services were identified and examined. The next step includes the identification of the social aspects of privacy that formulate trust on the Internet in order to capture a more holistic interdisciplinary view of this interesting field since the realization of trustworthy cloud services will increase both user trustworthiness and providers safety in the online world.

References

1. http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online
2. http://www.truste.com/us-consumer-confidence-index-2014
3. Hashizume K, Rosado DG, Fernández-Medina E, Fernandez EB (2013) An analysis of security issues for cloud computing. Journal of Internet Services and Applications 4: 1-13.
4. CSA Threats (2012) Top threats to cloud computing results update 2012. Cloud Security Alliance.
5. Pearson S (2013) Privacy, security and trust in cloud computing. In: Pearson S, Yee G (eds.). Computer Communications and Networks. Springer-Verlag, London. pp: 1-58.

6. Kalloniatis C, Mouratidis H, Manousakis V, Islam S, Gritzalis S, et al. (2014) Towards the design of secure and privacy-oriented Information Systems in the Cloud: Identifying the major concepts. Computer, Standards and Interfaces 36: 759-775.
7. https://www.huntonprivacyblog.com/2016/05/18/eu-council-adopts-the-network-and-information-security-directive/
8. David Burt (2009) Privacy in the cloud computing era, a Microsoft perspective. Microsoft Corp, Redmond, USA.
9. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
10. Yoon SJ (2002) The antecedents and consequences of trust in online purchase decisions. Journal of Interactive Marketing 16: 47-63.
11. Bedi P, Banati H (2006) Assigning user trust to improve web usability. Journal of Computer Science 2: 283-287.
12. Hoffman LJ, Lawson-Jenkins K, Blum J (2006) Trust beyond security: an expanded trust model. Communications of the ACM 49: 95-101.
13. Pavlidis M, Islam S, Mouratidis H, Kearney P (2014) Modelling trust relationships for developing trustworthy information systems. International Journal of Information Systems Modelling and Design 5: 25-49.
14. Bart Y, Shankar V, Sultan F, Urban GL (2005) Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. Journal of Marketing 69: 133-152.
15. Prieto AG (2009) From conceptual to perceptual reality: trust in digital repositories. Library Review 58: 593-606.
16. Kavakli E, Bantimaroudis F, Kalloniatis C, Gritzalis S, Avgeri K (2015) Towards the design of trustworthy websites for cultural organizations: a visitor's perspective, EMCIS 2015. 12th Mediterranean and Middle Eastern Conference on Information Systems, Greece.
17. Yan Z, Holtmanns S (2007) Trust modeling and management: from social trust to digital trust. In: Subramanian S (ed.), Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions. IRM Press, Hershey, PA. pp: 1-27.
18. Corritorea C, Krachera B, Wiedenbeckb S (2003) On-line trust: concepts, evolving themes, a model. Int J Human-Computer Studies 58: 737-758.
19. Cloud Computing. Academic Room.
20. Baburajan R (2011) The Rising Cloud Storage Market Opportunity Strengthens Vendors.
21. Kerravala Z (2016) Yankee Group, Migrating to the cloud is dependent infrastructure. Tech Target.
22. Voorsluys W, Broberg J, Buyya R (2011) Introduction to cloud computing. Cloud Computing: Principles and Paradigms 2011. John Wiley& Sons Inc. Publications. pp: 1-44.
23. http://www.cloudreviews.com/blog/what-is-hot-in-cloud-computing
24. http://www.businessweek.com/stories/2006-11-12/jeff-bezos-risky-bet
25. http://www.businessweek.com/stories/2008-08-04/cloud-computing-small-companies-take-flightbusinessweek-business-news-stock-market-and-financial-advice
26. Kuperberg M, Herbst NR, Kistowski JGV, Reussner R (2011) Defining and quantifying elasticity of resources in cloud computing and scalable platforms. Karlsruhe Reports in Informatics 16: 1-19.
27. Palmer M (2011) Economies of cloud scale infrastructure. Cloud Slam 2011, Burlingame, North America.
28. http://news.cnet.com/8301-13953_3-9977049-80.html
29. Wei J, Zhang X, Ammons G, Bala V, Ning P (2009) Managing security of virtual machine images in a cloud environment. ACM 11: 91-96.
30. Cannon JC (2004) Privacy: What developers and it professionals should know. Addison-Wesley.
31. Fischer HS (2001) IT-Security and privacy, design and use of privacy enhancing security mechanisms. Springer-Verlag, Berlin Heidelberg.
32. https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf