Building Trust in the Cloud Environment: Towards a Consumer Cloud Trust Label

Lisa van der Werff, Theo Lynn, HuanHuan Xiaong, Graham Hunt, John Morrison, Philip Healy, David Corcoran

Irish Centre for Cloud Computing and Commerce
Dublin City University
Dublin 9, Ireland
e-mails: {lisa.vanderwerff@dcu.ie, theo.lynn@dcu.ie, huanhuan.xiong@dcu.ie, graham.hunt@.dcu.ie, j.morrison@cs.ucc.ie, p.healy@cs.ucc.ie, david.corcoran22@mail.dcu.ie}

Abstract— **Low consumer trust presents a significant barrier to cloud service adoption and the growth of the cloud industry. The cloud environment is generally perceived to have high levels of uncertainty and risk. Trust plays a central role in allowing consumers to overcome this risk when making adoption decisions. This paper discusses the characteristics of cloud services that form the basis for consumer trust decisions and argues that service providers need a more transparent, accessible method of communicating these characteristics to potential consumers. As such, this paper is directly relevant to conference tracks discussing consumer-oriented digital services and in particular the topic of consumer trust in digital society. Drawing on the nutrition label concept and aspects of previous computational trust models, we propose a dynamic trust label for cloud computing. The cloud trust label aims at present real time and cumulative metrics to consumers in an easily understandable format. In doing so, the label can be used to aid knowledge based trust decisions and ultimately encourage adoption of cloud services.**

Keywords-cloud computing; trust; nutrition label; risk.

I. INTRODUCTION

Cloud computing can be described as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (National Institute of Standards and Technology, NIST [1]). The information technology (IT) related savings for cloud computing include lower implementation and maintenance costs; cost of power, cooling, storage and paying only for what is used [2]. There are also operational benefits due to the flexibility and agility of cloud computing. According to the European Commission, cloud computing has the potential to generate €250 billion in gross domestic product (GDP) with the creation of 2.5 million jobs by 2020 [3].

A number of factors are cited as barriers to wider cloud adoption by consumers. These include issues with trust, security and transparency [4], which introduce high levels of risk and uncertainty and prevent more widespread cloud adoption. Improving our understanding of the factors underlying consumer trust decisions is vital to capitalising on the potential benefits of cloud computing.

Previous research aimed at improving trust in the Cloud has focused predominantly on technical aspects of data handling and assigning accountability for potential issues to specific parties in the chain of service provision [5]. This focus emphasises methods of preventing and handling trust violations but fails to explain the role of consumer expectations and perceptions in driving their initial trust and adoption decisions. This paper takes a consumer-oriented view of trust in cloud computing and examines the risks inherent in the cloud environment and the characteristics of cloud technology which consumers are likely to assess in making trust judgements. Building on work done on nutrition labels and computational trust models, we propose the use of a trust label for cloud computing that will allow Cloud Service Providers (CSPs) to signal dynamic trustworthiness information to consumers.

The remainder of this paper is organised into three sections. First, we will discuss issues of risk and uncertainty in the cloud environment including the selection of CSPs, the characteristics of cloud computing and the legal issues which impact consumer cloud experiences. Second, we will explore the theoretical underpinning of consumer trust perceptions and provide a brief overview of relevant literature on trust in the field of information systems. Finally, we examine previous research into the use of nutrition labels to communicate information in the context of information systems and outline our plans to develop a label specific to developing trust within the Cloud industry.

II. RISK AND UNCERTAINTY IN THE CLOUD ENVIRONMENT

Cloud computing provides compelling benefits and cost saving options for consumers [4]. However, adopting cloud computing services presents new risks and uncertainty that increases the perceived complexity of the adoption decision-making process and cloud provider selection [2]. The Cloud can introduce a single point of failure as demonstrated by Amazon EC2 outage in 2011 [6] and raises concerns over the security of data as demonstrated by the recent

 ISBN: 978-1-61208-324-7

controversy over NSA surveillance [7]. CSPs need to look for mechanisms that can address such risk factors.

In adopting cloud services, the user is making a commitment to a CSP and needs to understand the possible impact of selecting the wrong CSP, security and data privacy risks that are inherent in the cloud environment, as well as the legal issues that are currently leading to uncertainty.

A. *Cloud Service Provider Selection*

For enterprise consumers, the economic appeal of adopting cloud computing is often depicted as "converting capital expenses to operating expenses" [8]. The perceived benefit is that by removing the up-front capital expense the user transfers the risk of overprovisioning or underprovisioning and frees up capital for core business activities [8]. However, accurately comparing CSP's pricing schemes can be challenging with providers using different pricing models making the selection process difficult [9]. Although cloud computing is cost effective and cost transparent, incorrect CSP selection will lead to a user paying more than expected [9]. Consumers can easily become locked-in and dependent on a vendor such that they cannot terminate the relationship without incurring substantial financial costs [10]. This is a significant concern for consumers as it reduces their flexibility to move between CSPs and reduces the consumer's bargaining power [11]. CSPs will often design lock-in into their services through the use of closed architectures to reduce portability and ease of data migration [11]. As a result, selecting a CSP is most likely the beginning of a long-term relationship that will be difficult to break.

B. *Cloud Computing Characteristics*

The five essential characteristics of cloud computing as set out by NIST [11]: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service suggest flexibility and ease of use for the consumer. However, these characteristics convey a contradictory message in the context of technology decision-making by introducing new risks and uncertainty [5]. For example, in outsourcing to a CSP the consumer faces similar concerns to those involved in a traditional outsourcing decision whereby they are limiting their control over the service while still retaining responsibility for it [5]. They are paying for a measured service yet have no control over its measurement. Hosting application and data in a multi-tenant environment increases consumer uncertainty related to privacy, compliance, integrity and confidentiality among other concerns [2].

C. *Legal Issues*

As a result of lack of consumer control over cloud resources, they must rely on contracts or other formalised trust mechanisms to try encourage appropriate usage [5]. It has been suggested that the contract between the consumer and CSP can often lead to further uncertainty [11]. One of the difficulties is that existing legislation was not written with the Cloud in mind [11]. A number of common legal issues are outlined below.

- **Security and Data Protection** are continually ranked among the top barriers to cloud adoption [2][4]. For many consumers, the perceived risk is still too high to place critical personal information in the Cloud. Possible risks include increased vulnerability of data being accessed by third parties through surveillance by national security agencies, malicious users, data leakages, failure of electronic and physical transport systems for data and back up (if carried out) [2]. In many cases, legal agreements for cloud services seek to place the responsibility for security and data protection on the data owner, i.e., the consumer, to ensure a level of security appropriate to the risks represented by the processing of the data [11][12]. Another factor causing uncertainty is many standard terms of CSPs do not necessarily require security incidents to be reported to the consumer [13]. Consumers must also consider the security and location of their data while in transit. Many cloud legal agreements specify that data will be stored and processed within certain regions but do not specify that they will not be transferred outside these limits [11].

- **Service Levels and Performance** – The Service Level Agreement (SLA) will typically contain a defined list of services delivered, performance targets, auditing mechanisms and any compensatory mechanisms [11]. However, uncertainty is introduced as many SLAs rely on the chain of service provision; this may mitigate any commitment by the CSP to performance [11]. Many CSPs, typically, reserve the right to amend contract terms unilaterally where continued use is deemed acceptance resulting in continued uncertainty for the consumer [14]. Often consumers cannot monitor performance levels and are reliant on information provided by the CSP [11].

- **Data integrity** refers to maintaining and assuring the accuracy and consistency of data over its life cycle [15]. Many consumers consider the Cloud as a safe method of backing up their data. As a result, data integrity is core to consumer expectations [11]. A recent study found that the majority of CSPs place the legal responsibility for preserving the data integrity with the client increasing their potential risk [14].

- **Choice of jurisdiction** – The nature of cloud computing assumes that data will be stored across multiple data centres by a CSP introducing a degree of jurisdictional uncertainty even if stated in the contract [11]. With almost 50 per cent of CSPs choosing US

 ISBN: 978-1-61208-324-7

jurisdiction, there is a disincentive for consumers to take legal action due to the high costs of dispute resolution [11]. In many cases, CSPs that choose a US state as applicable law seek to deny any liability for damage as far as possible and restrict compensation to service credit [14]. This can result in significant financial losses for the consumer. However, it should be noted that EU law, typically, does not allow providers to contractually avoid liability to the extent of the US legal system.

- **Termination** – A commonly cited issue for consumers is the ability to retrieve and transfer their data on leaving the CSP [11]. Most providers fail to provide assistance in off boarding data and those that do tend to charge for it. This increases the chances of a consumer becoming locked-in to the CSP. Furthermore, the standard terms of the contract often provide little grace period for consumers to migrate their data [11].

To increase cloud adoption, the above risks and uncertainty need to be addressed.

III. SIGNALLING TRUST IN THE CLOUD

In contexts where individuals perceive high levels of risk and uncertainty, trust provides a vital basis for interdependence and cooperation between two parties in a relationship [16]. Indeed the existence of risk is a necessary condition of trust in another party. Improving consumer trust in cloud services provides an important opportunity for consumers themselves, and for the cloud industry as a whole, in overcoming high levels of risk and uncertainty and paving the way for cloud adoption.

Trust is considered a three stage process consisting of the forming of positive expectation, the decision to make oneself vulnerable to another party and a risk taking act [17]. This sequencing of events has important implications for the approach that cloud service providers might take to increasing consumer trust and reducing perceptions of risk and uncertainty in the cloud environment. In order to encourage cloud adoption, which might be seen as a risk taking behaviour, providers must focus on how to increase positive expectations (stage 1) and drive consumer willingness to be vulnerable (stage 2) despite the risks perceived in their environment.

A considerable body of literature in the field of interpersonal and organisational trust has been devoted to uncovering the factors which contribute to positive trust expectations. The dominant model in the trust literature was put forward by Mayer et al. [18] and proposes that expectations consist of trustworthiness perceptions formed on the basis of the perception of characteristics of the other party. Specifically, three key characteristics are assessed: ability – the competence, knowledge and skills of the other party; benevolence – the extent to which the other party is expected to act in the trustor's interests; and, integrity – the other party's adherence to a set of acceptable principles and rules.

Although this model was originally designed to capture the interpersonal trust process, it has proven to be robust across levels of analysis [19] and is frequently applied to improving our understanding of trust in organisations across a range of industries. A small body of literature has recently developed and adapted the trustworthiness model to the context of trust in technology [20][21]. The primary difference in this context is that the party in which trust is placed is incapable of consciousness or moral agency which prevents it for example from making a decision about whether or not to behave in a benevolent manner [22]. However, trust is a psychological state [23] that exists in the mind of the trustor. Accordingly, theorists [22] suggest that interpersonal theories of trust are useful in understanding trust relationships between humans and technology as long as the human party is making the trust assessments and decisions. In other words, it is logical to apply existing trust theory to understand humans trusting technology but not vice versa.

The traditional trustworthiness model of ability, benevolence and integrity has been adapted in the information systems literature to provide a more suitable assessment of the trustworthiness characteristics of an IT artefact [20][22]. It is suggested that assessments of trustworthiness in this context are built on consumer perceptions of performance, helpfulness and predictability [22]. Performance relates easily to the original dimension of ability in that it refers to the consumer's perception of the competence of the product and its ability to help them to carry out the required task. Helpfulness is proposed as a substitute for benevolence and describes the consumer's perception that support in the use of the product is available. Finally, predictability, related to the original dimension of integrity, refers to the consumer's perception that they can both understand and predict the behaviour of the technological product. Together knowledge and perception of these three characteristics provide a basis for consumer trust in technology.

Trust built on knowledge of the characteristics of a cloud service has an important advantage over trust built on a simple calculation of the risks and benefits of cloud product adoption. Knowledge based trust is likely to be less suspicious and fragile than that based on pure calculation of potential costs and benefits [24][25]. Building robust trust relationships with consumers is advantageous for cloud service providers as it allows a greater threshold for the acceptance of small violations of consumer expectations. Knowledge based trust is also advantageous for cloud consumer as once the trust relationship is established less time is needed for the vigilant monitoring of the service allowing users to fully realise the benefits of the service. However, the online environment is a context in which an overwhelming array of information is available to consumer. Although consumers are motivated to evaluate the trustworthiness of information they access online, the thoroughness of this evaluation is limited by time and cognitive resource constraints. In order to realise the benefits associated with trust, the challenge for the cloud industry lies in devising an effective means of communicating trustworthy characteristics to the consumer. For a thorough review of trust in online environments see Grabner-Krauter and Kalushcha [26] and Beldad et al. [27].

Computational trust models have existed in the field of information systems for many years, typically known as reputation mechanisms [28]. Information related to past behaviours of users is used to determine the reputation of those users in terms of availability, reliability, good quality and security. The mechanism is generally implemented based on a centralized rating model so that the customers and sellers can rate each other using numerical scale or feedback comments (e.g., Amazon, eBay, Taobao, etc.).

Within the cloud computing literature, researchers are beginning to recognize the need for a mechanism to build consumer trust in the Cloud. The traditional reputation mechanism has been extended to distributed systems to meet the challenges of cloud computing [29]. Vu et al. proposed peer-to-peer (P2P) web service discovery that uses Quality of Service (QoS) data and user feedback to rank and select services [30]. The use of SLAs and business activities monitoring is suggested as a method to guarantee the quality of cloud services [31]. In a similar vein, Bogataj and Pucihar suggest a trust building mechanism for cloud computing adoption, which consists of authentication, system security, service quality and non-repudiation [32]. Lynn et al. [33] recently outlined the use of a trustmark to help consumers of cloud computing to build trustworthiness. Trustmarks typically involve one or more of six elements: a declaration of best practice, a subscription to a code of conduct, scrutiny for membership, sanctions for failure, recourse for wrongful revocation, and a remedy for aggrieved customers [33]. They are proposed to build trust by providing evidence of third party certification and have been demonstrated as an effective mechanism for increasing credibility and consumer trust online [34].

IV. A NUTRITION TRUST LABEL FOR CLOUD COMPUTING

In the United States, a Nutrition Labelling and Education Act (NLEA) [35] was signed into law in 1990 that gives the Food and Drug Administration (FDA) [36] authority to require nutrition labelling of the majority of food products. The purpose of the food nutrition label is to play a role in informing consumers about their food purchasing decisions by supporting and supplementing other nutrition education strategies [37]. For instance, offering nutrient content claims and certain health messages, providing quantitative information about nutrients and making it easy to compare between a small set of items. The provision of Nutrition information on food packaging allows consumers to make more informed decisions about their nutrition and adapting their purchase behaviour to suit their individual dietary needs [38]. The typical nutrition label is shown in Figure 1.

The nutrition labelling mechanism has gained wide recognition around the world, and built a broader understanding of practices used in designing and defining labelling requirements [39].

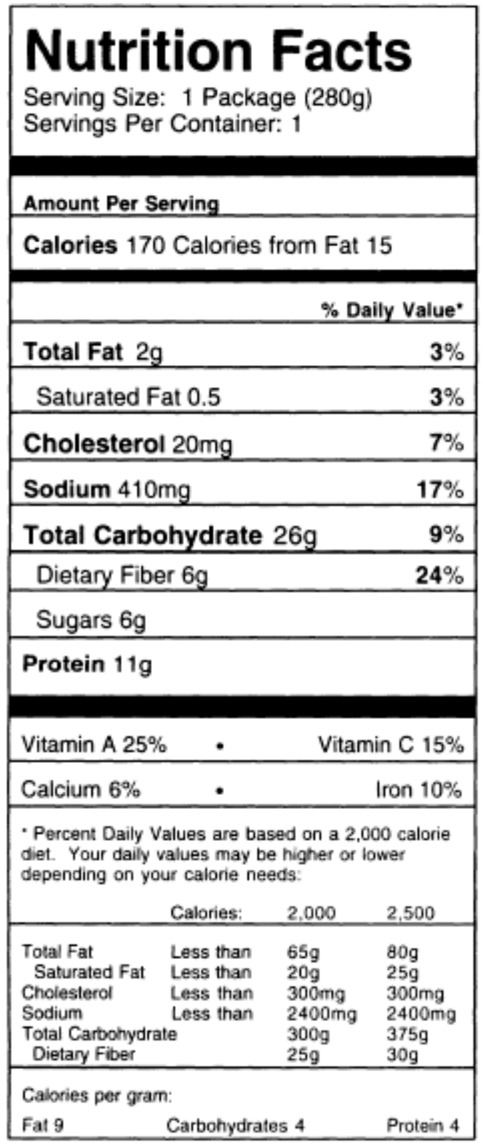

Figure 1. the Food and Drug Administration's Nutrition Fact panel as regulated by the NLEA, [41]

Carnegie Mellon has demonstrated the transferability of the nutrition label concept to the technology industry in their recent development of a privacy nutrition label [39]. Their work builds on the Platform for Privacy Preferences (P3P) expandable Grid that presents a "nutrition facts" pattern where consumers can investigate and explore the privacy policy of websites [40]. P3P was created by the World Wide Web consortium for encoding and sharing online privacy policies in a standard format (i.e., XML Schema Definition Standard), which can be retrieved automatically and interpreted easily by consumers [42]. Drawing on this, a privacy nutrition label was proposed aiming to simplify the P3P Expandable Grid to enhance user experience by reducing clutter and simplifying symbols [39]. An early stage, simplified label is shown in Figure 2.

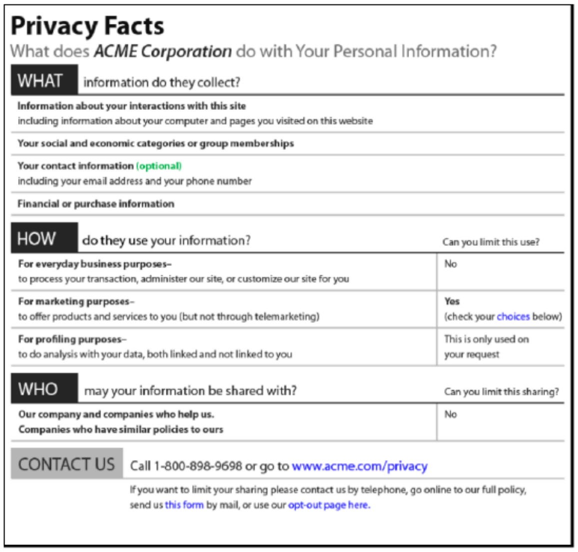

Figure 2. the simplified Privacy Nutrition Label, [39]

CMU's proposed Privacy Nutrition Label represents three main concerns:

- **What** kind of information is collected, such as IP address, email address, name.
- **Who** will share or use this information, such as current company or third party.
- **How** this information is used, such as regular navigation, tracking, personalization or telemarketing.
- **Contact Information** to allow the user to obtain further information and support.

CMU's privacy nutrition label provides a good example of how the nutrition label concept increases clarity and availability of information in a technology context. As such, it provides a useful basis for how we might develop a label specific to developing consumer trust in CSPs. However, a number of important questions still remain. It is not yet clear how people will use the label in practice or what quantifiable information provides the best basis for consumer decision-making. In addition, thus far nutrition labels are typically presented as a static representation or logo. In the context of cloud computing, access to real time metrics provides a unique opportunity to present consumers with a continuously updating, dynamic label. Building on this foundation, we propose the use of the nutrition label concept to design a trust label for cloud computing to provide clarity and greater consumer access to information on which to base trust and adoption decisions.

V. THE IC4 CLOUD TRUST LABEL PROJECT

In November 2013, the Irish Centre for Cloud Computing and Commerce (IC4) established a research project to develop and test such a trust label. This project seeks to use a qualitative online Delphi study of cloud industry experts and users to determine the most appropriate format for a cloud trust label, and establish how the risks discussed in Section II can be overcome. The project comprises five rounds of anonymous online interaction between the industry experts and users:

- **Round 1 - Brainstorming:** Discussion to be focused on brainstorming label content.
- **Round 2 – Identifying Label Features:** Finalising a list of label content and discussing the optimal way to communicate this to users.
- **Round 3 – Label Refinement:** Presentation of a draft label design for discussion by the group.
- **Round 4 – Final Label Distribution:** Discussion of label refinement following Round 3.
- **Round 5 – Evaluation:** Evaluation of the final label and process.

Once consensus on label has been agreed, a further research project will be conducted to empirically examine the impact of the label on consumer trust expectations and decisions and to investigate their impact on cloud adoption rates. The theoretical potential of the cloud trust label is clear. However, as consumer perceptions are key, demonstrating the label's practical significance and utility in terms of actual impact on consumer attitudes will be a vital step towards encouraging widespread adoption by CSPs. Separate research on technical systems for monitoring, transferring, analysing and surfacing cloud service data to the trust label securely is required. In particular, attention needs to be given to how the monitoring and analysis performed to calculate the trust metrics can be made minimally intrusive and tamper evident. Finally, consideration will need to be given to the best way of deploying the label and encouraging CSPs to display and communicate this information. Providing convincing evidence of the practical utility of the label for both experts and non-experts will be central to this process. In addition, the label will provide an important benefit to quality service providers by providing an easier means of comparison across services and a clear map of how CSPs might differentiate themselves from their competition.

VI. CONCLUSION

This paper proposed a trust label as a means for cloud service providers to communicate trustworthiness to consumers. In the cloud environment, consumers encounter high levels of risk and uncertainty when making decisions about adopting cloud products. Trust theory suggests that

 ISBN: 978-1-61208-324-7

cloud adoption behaviours will be based on consumer knowledge of trustworthiness characteristics that provide a foundation for trust decisions. The effective communication of these characteristics to consumers is vital to improving trust in the cloud environment and maximizing cloud adoption. The dynamic nutrition trust label proposed in this paper provides a means of meeting this communication need. Future research will address the specific content and features of the label and empirically examine its impact on consumer trust and cloud adoption practices.

REFERENCES

[1] P. Mell and T. Grance, “The NIST definition of Cloud Computing,” National Institute of Standards and Technology, U.S Department of Commerce, 2011

[2] M. Carroll, A. Van der Merwe, and P. Kotze, “Secure cloud computing: Benefits, risks and controls,” Information Security South Africa (ISSA), IEEE, August, 2011, pp. 1-9.

[3] European Commission, “Unleashing the potential of cloud computing in Europe” 2012

[4] D. Bradshaw, G. Folco, G. Cattaneo, and M. Kolding, “Quantitative estimates of the demand for cloud computing in Europe and the likely barriers to up-take” IDC, 2012.

[5] S. Pearson, and A. Benameur, "Privacy, security and trust issues arising from cloud computing." Cloud Computing Technology and Science (CloudCom), IEEE, 2010, pp. 693-702.

[6] J. Pepitone, “Amazon EC2 outage downs Reddit, Quora,”Available: http://money.cnn.com/2011/04/21/technology/amazon_server_outage/, 2011 [retrieved: February, 2014].

[7] G. Greenwald and E. MacAskill, “NSA Prism program taps in to user data of Apple, Google and others,” Available: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, 2013 [retrieved: February, 2014].

[8] A. Fox et al., “Above the clouds: A Berkeley view of cloud computing,” Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS, 28, 2009.

[9] U. Onwudebelu and B. Chukuka, “Will adoption of cloud computing put the enterprise at risk?” Adaptive Science & Technology (ICAST), IEEE 4th International Conference, pp. 82-85, October 2012.

[10] K. Zhu and Z. Zhou, “Lock-in strategy in software competition: Open-source software vs. proprietary software,” Information Systems Research, 2011, pp. 1- 10.

[11] T. Leimbach, D. Hallinan, A. Weber, M. Jaglo, L. Hennen, M. Nentwich, S. Strauß, R. Øjvind Nielson, T. Lynn, and G. Hunt. (2013) “Impacts of Cloud Computing. Bericht-Nr. Deliverable No.3 of the STOA Project European Perspectives on impacts and potentials of Cloud Computing and Social Network Sites (Interim Report – Phase III)”, Science and Technology Options Assessment, European Parliament.

[12] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[13] W. Hon, C. Millard, and I. Walden, “Negotiating cloud contracts: Looking at clouds from both sides now,” Stanford Law Review, vol. 16(1), 2012, pp. 79-129.

[14] S. Bradshaw, C. Millard, and I. Walden, “Contracts for clouds: comparison and analysis of the terms and conditions of cloud computing services.” In International Journal of Law and Information Technology, vol. 19(3), 2011, pp 187-223.

[15] J. E. Boritz, “IS practitioners' views on core concepts of information integrity,” International Journal of Accounting Information Systems, vol. 6(4), 2005, pp. 260-279.

[16] P. P. Li, "Towards an interdisciplinary conceptualization of trust: A typological approach," Management and Organization Review, vol 3(3), 2007, pp. 421-445.

[17] B. McEvily, V. Perrone, and A. Zaheer, “Special issue: Trust in an organizational context. Organization Science,” vol. 14(1), 2003.

[18] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust." Academy of Management Review, vol. 20(3), 1995, pp. 709-734.

[19] F. D. Schoorman, R. C. Mayer, and J. H. Davis, "An integrative model of organizational trust: Past, present, and future," Academy of Management Review, vol. 32(2), 2007, pp. 344-354.

[20] D. H. McKnight, M. Carter, J. B. Thatcher, and P. F. Clay, “Trust in a specific technology: An investigation of its components and measures,” ACM Transactions on Management Information Systems (TMIS), vol. 2(2), 2011, pp. 12-33.

[21] M. Söllner, A. Hoffmann, H. Hoffmann, and J. M. Leimeister, “Towards a theory of explanation and prediction for the formation of trust in IT artifacts,” In 10th Annual Workshop on HCI Research in MIS, Shanghai, China, December, 2011, pp. 1-6.

[22] M. Söllner, P. Pavlou, and J. M. Leimeister, “Understanding trust in it artifacts – A new conceptual approach,” Academy of Management Proceedings in Florida, USA, August 2013.

[23] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, “Not so different after all: A cross-discipline view of trust,” Academy of Management Review, vol. 23(3), 1998, pp. 393-404.

[24] R. J. Lewicki and B. B. Bunker, “Developing and maintaining trust in work relationships,” Trust in Organizations: Frontiers of Theory and Research, Thousand Oaks, CA: SAGE Publications, Inc., 1996, pp. 114-139.

[25] G. Dietz, “Partnership and the development of trust in British workplaces,” Human Resource Management Journal, vol. 14(1), 2004, pp. 5-24.

[26] S. Grabner-Krauter and E. A. Kaluscha, “Empirical research in on-line trust: a review and critical assessment,” International Journal of Human-Computer Studies, vol 58, 2003, pp. 783-812.

[27] A. Beldad, M. de Jong, and M. Steehouder, “How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust,” Computers in Human Behavior, vol 26, 2010, pp.857-869.

[28] J. Sabater and C. Sierra, “Review on computational trust and reputation models,” Artificial Intelligence Review, vol. 24(1), 2005, pp. 33-60.

[29] P. Resnick and R. Zeckhauser, “Trust among strangers in Internet transactions: Empirical analysis of eBay’s reputation system,” Advances in Applied Microeconomics: A Research Annual, vol. 11, 2002, pp. 127-157.

[30] L. H. Vu, M. Hauswirth, and K. Aberer, “Towards P2P-based semantic web services discovery with QoS support,” Workshop on Business Processes and Services (BPS), in conjunction with the Third International Conference on Business Process Management, Nancy, France, September 2005.

[31] M. Alhamad, T. Dillon, and E. Chang, “SLA-based trust model for cloud computing,” 13th International Conference on Network-Based Information System, pp. 321-324. Takayama, Japan, September 2010.

[32] K. Bogataj and A. Pucihar, “Business model factors influencing cloud computing adoption: Differences in opinion,” 25th Bled eConference Doctoral Consortium, Bled, Slovenia, June 2012.

[33] T. Lynn, P. Healy, R. McClatchey, J. Morrison, C. Pahl, and B. Lee, “The case for cloud service trustmarks and assurance-as-a-service,” 3rd International Conference on Cloud Computing and Services Science Closer'13, Aachen, Germany, May 2013.

[34] K. D. Aiken and D. M. Boush, “Trustmarks, objective-source ratings, and implied investments in advertising: Investigating online trust and the context specific nature of internet signals,” Journal of Academy of Marketing Science, vol. 34(3), 2006, pp. 308-323.
[35] Nutrition Labeling and Education Act (NLEA) Requirements, Available: http://www.fda.gov/iceci/inspections/inspectionguides/ucm074948.htm, 1994 [retrieved: February, 2014].
[36] FDA, “Labeling & Nutrition”, U.S. Food and Drug Administration, Available: http://www.fda.gov/Food/IngredientsPackagingLabeling/LabelingNutrition/default.htm, 2013 [retrieved: February, 2014].
[37] R. Rothman, R. Housam, H. Weiss, D. Davis, R. Gregory, T. Gebretsadik, A. Shintani, and T. Elasy, “Patient understanding of food labels: the role of literacy and numeracy”. American Journal of Preventive Medicine, vol. 31(5), 2006, pp. 391-398.
[38] A. Gracia, M. Loureiro, and R. M. Nayga Jr., "Do consumers perceive benefits from the implementation of a EU mandatory nutritional labelling program?" Food Policy, vol. 32(2), 2007, pp. 160-174.
[39] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder, “A ‘Nutrition Label’ for privacy,” Symposium on Usable Privacy and Security (SOUPS), Mountain View, CA, USA, July 2009.
[40] R.W. Reeder, “Expendable grids: A user interface visualization technique and a policy semantic to support fast, accurate security and privacy policy authoring,” PhD thesis, Carnegie Mellon, Available: http://www.robreeder.com/pubs/ReederThesis.pdf , 2008 [retrieved: February, 2014].
[41] S. B. Keller, M. Landry, J. Olson, A. M. Velliquette, S. Burton, and J. C. Andrews, “The effects of nutrition package claims, nutrition facts panels, and motivation to process nutrition information on consumer product evaluations,” Journal of Public Policy & Marketing, vol. 16(2), 1997, pp. 256-269.
[42] W3C, the Platform for Privacy Preferences 1.1 (P3P1.1) Specification, Available: http://www.w3.org/TR/P3P11/, 2006 [retrieved: February, 2014].

 ISBN: 978-1-61208-324-7