End-User Perceptions of Safety and Trust in Cloud Computing Platforms

Tristan K. O’Dwyer, MBA, Anglia Ruskin University
odwyertristan@gmail.com

Abstract:

Cloud computing platforms offer many advantages to businesses and consumers in terms of reduced costs, flexibility and the accessibility of data. However, concerns remain about the security of data stored in the cloud. This paper investigates some of the technical issues surrounding data security in the cloud and examines the available literature for solutions. Moreover, it builds on a conceptual framework regarding the role of trust in the decision to use cloud services, end-user attitudes to risk and the relationship between provider reputation and trust. In line with previous research in this area, the study found a high perception of risk among users of cloud services, and an ambiguous attitude to positive statements about trust in the security of cloud platforms. The results of the study also suggest that provider reputation correlates strongly with trust and that trust is a driver of intention to use cloud service.

Keywords: Cloud computing, data, trust, provider reputation, risk, security

INTRODUCTION

Cloud computing is a form of utility computing (Buyya et al, 2009) which utilizes remote servers to offer centralised data storage (Velte et al, 2010). Cloud computing services have the characteristics of a utility in that they are location-independent and available on demand and are often sold on a usage model, similar to traditional utilities such as electricity and telephone services (Strommen-Bakhtiar and Razavi, 2011).

Cloud computing is thought to offer numerous advantages to businesses and consumers in terms of cost efficiencies, back-up and recovery, and storage and integration (Marston et al, 2011). Cloud computing “is a disruptive technology with profound implications...for the IT sector as a whole” (Dikaiakos et al, 2009, p. 10), and which is fast becoming the dominant paradigm in computing (Chen et al, 2010; Young et al, 2011).

In spite of its many advantages and increased popularity, cloud computing introduces a new set of security concerns and risks to data and privacy (Catteddu, 2010; Carlin and Curran, 2011; Chen, 2012). Zissis and Lekkas (2012) argue that the shared nature of the infrastructure associated with cloud computing, which on one hand makes it attractive and cost effective, also represents a vulnerability. They point out that as the separation of drives in cloud architecture is virtual it lacks the security of hardware separation and is potentially prone to data remanence, where nominally erased is still accessible.

The risks associated with data security in cloud computing are well known, documented and discussed in the literature (Jensen et al, 2009; Grobauer et al, 2010; Gruschka and Jensen, 2010; Hamlen et al, 2010; La’Quata, 2010; Zhou et al, 2010; Jansen and Grance, 2011; Kshetri, 2013). Technical solutions are available and deployed, and significant portions of the literature suggest that security in cloud computing platforms is more sophisticated that the measures employed by
individuals and small and medium enterprises (Dorey and Leite, 2011; Kevin, 2014).

However, in spite of the widespread availability of technical solutions to data security issues, and a widespread view among experts that concerns about data security are misplaced (Viega, 2012; Mell, 2012), previous research suggests that many end-users and potential end-users of cloud platforms exhibit a lack of trust in data security measures and perceive the use of cloud platforms as risky (De Felice, 2010; Alijani et al, 2014; Burda and Teuteberg, 2014), which in turn has a negative effect on the take-up of services (Benlian et al, 2009; King and Raja, 2010; Pearson, 2011).

Building on previous research, this paper examines the issue of trust in the security of cloud platforms and the perception of risk among end-users. Specifically, this paper offers the following hypotheses:

H1: Users of cloud computing platforms exhibit trust in cloud platform providers.

H2: Users of cloud computing platforms perceive the use of cloud computing platforms to be risky.

Additionally, the paper seeks to establish the influence of perceived risk on the take up of cloud services, and the role of provider reputation in building trust, and asks the following research questions:

R1: Does provider reputation influence trust?

R2: Does perceived risk influence intention to use cloud computing platforms?

Literature Review

Technical Aspects

Kevin (2014) offers an argument in favour of cloud security which suggests that the security measures in place by cloud computing vendors are often better than those in place at a local level, especially in smaller businesses. Viega (2012, p. 3) calls concerns about data security in cloud platforms a “misconception”, while Mell (2012) argues that many of the concerns about data security are not unique to cloud computing. Dorey and Leite (2011) argue that cloud platforms can have a positive effect on data security, firstly because they put data into the hands of a security-conscious provider, but also because they prevent the entire network stack being exposed to attack. They also argue that because cloud providers have multiple clients, they are better placed to observe a wider pattern of attacks and security threats than a single client. Kaufman (2009), on the other hand, voices the concern that outsourcing data to cloud providers’ makes data-owners feel that they can wash their hands of responsibility for security.

Denz and Taylor (2013) write that the security community is implementing a wide range of technical tools to increase security, including cloud resilience and malware prevention, but they argue that the industry approach is too disjointed to be effective.

While there is a feeling among IT professional that technical developments have increased the security of data in the cloud (Neff, 2012; Khansa and Zobel, 2014) and finding comprehensive technical solutions to data security issues remain an industry priority, Mitropoulos (2013) performed penetration tests on seventy virtual machines running on Amazon EC2, finding only twenty-six of these to be secure. Similarly, Teneyuca (2011, p. 102) calls cloud computing security “an illusion”; while Green (2013), suggests that we should simply not expect cloud computing to be secure.

Gonzalez et al (2012) conducted an analysis of the security concerns about cloud computing across a wide range of academic literature, white papers and security reports to identify the common security concerns and potential security. Their analysis concluded that while the security concerns were relevant and shared across the industry and academia, an almost equal amount of solutions were already available to address these concerns. This would suggest that cloud computing platform providers are aware of, and sensitive to, concerns about data security.

Muttik and Barton (2009) explain that the cornerstone of computer security, anti-virus software, is still fundamentally the same as when they were first developed in the 1980s, and that they must adapt
if they are to offer sufficient security to cloud platforms, while Nauwelaerts and Le Bousse (2009) also agree that new approaches to security are needed to ensure the security of data in the cloud.

**Specific Security Issues**

**Data Security**

Subashini and Kavitha (2011) identify a number of security elements impacting on the security of data in cloud computing services and in the software-as-a-service model in particular. The first of these elements is data security. Subashini and Kavitha point out that in traditional on-premise systems the data owner has full control over the physical location and access control policies, whereas in a cloud system these become the responsibility of the provider. Bulgurcu (2010) points out that one of the single biggest sources of data security risk is non-compliance with security policies by employees and the idea that human error poses a large threat to data security is well established in the literature (Huston, 2001; Kumar, 2009). In relinquishing control of security policies to a third party, organisations have no say in the human management of their data, and are therefore less able to control the human element of data risk.

He et al (2014) point out that the shared physical nature of cloud architecture leads to network security issues and cloud computing systems are inherently vulnerable to Denial of Service attacks (Chonka et al, 2012).

**Web Application Security**

Web applications are thought by some to be particularly vulnerable to security threats (Maguire and Miller, 2010), because the short development times do not allow for the total elimination of security flaws (Huang et al, 2003) and indeed security requirements for web applications are often not even considered at the requirements gathering stage (Salini and Kanmani, 2012). The idea that security requirements in web applications are sometimes ignored or not considered properly at the design stage is shared by Brown et al (2012).

**VIRTUALIZATION SECURITY**

Virtualization in this context refers to the use of software to create multiple virtual machines on a single piece of hardware (Pearce et al, 2013).

Cohen (2010) argues that virtualization enhances security as it provides for complete OS separation. Shackleford (2010), concedes that while virtualization platforms can be prone to security flaws, it is relatively easy to overcome these issues with appropriate planning. However, others hold that virtualized systems cannot be secured in the same way as hardware systems and are inherently more vulnerable (Perez et al, 2008; Vaughan-Nichols, 2008; Tsai et al, 2011). Chowdhury and Boutaba (2010, p. 872) point out that a “denial-of-service (DoS) or a distributed DoS (DDoS) attack against the physical network in a virtualized environment will affect all the virtual networks hosted on that network”

**TECHNICAL SOLUTIONS**

**ENSURING WEB APPLICATION SECURITY**

Razzaq et al (2014) propose an approach to web application security using semantic rules to prevent attacks, which they claim is more secure than signature-based methods of security.

Numerous tools exist to test and ensure the security of web applications. These include , source code analyzers, black-box scanners, database scanners and binary analysis tools (Curphey and Arawo, 2006)

**Ensuring Virtualization Security**

The traditional methods of ensuring virtualization security in the cloud are firewalls and anti-virus software, although these methods have their shortcomings (Manavi et al, 2012)

Lombardi and Di Pietro (2011) propose an Advanced Cloud Protection System (ACPS) which they claim provides protection from most forms of attack.
END USER PERCEPTIONS OF SAFETY AND TRUST IN THE CLOUD

THEORETICAL FRAMEWORK

In a study of Certified Public Accountants considering switching to cloud services, DeFelice (2010) found that security issues, alongside reliability issues, were a primary concern, while research by Aijani et al (2014) found that just 59% of small businesses were satisfied with the security levels of cloud platforms.

The issue of end-user trust in cloud computing platforms is a recurring motif in the literature on cloud computing (Pearson and Benameur, 2010; Roberts and Al-Hamadi, 2011; Burda and Teuteberg, 2014; Nanavati et al, 2014; Adjei, 2015) and earning the trust of end-users remains a “critical challenge for the cloud computing industry” (King and Raja, 2010, p. 308), while a number of studies have found that a lack of trust in cloud security has a negative effect on the take up of cloud services amongst businesses (Benlian et al, 2009; Pearson, 2011)

Ryan and Falvey (2012) argue that the lack of trust in cloud computing platforms is misplaced, and the perception of lack of security simply stems from a perceived lack of control by the end user. In a similar fashion, Srinivasan (2010) claims that in the case of small businesses in particular, the security measures offered by cloud vendors are better than anything the business could provide themselves.

Given the amount of technical solutions in place and in development to ensure data security in cloud platforms, and the view that cloud providers are often in a much stronger position than end users to ensure data security, it would appear that concerns about the security of data security in the cloud is based on more abstract issues of trust than on concrete technical considerations, something Payne (2013) suggests that cloud vendors can overcome through increased transparency and support procedures.

Burda and Teuteberg (2014) see the issue of trust in cloud computing services in terms of a technology acceptance model (Davis, 1989). While the original 1989 model proposed by Davis was primarily concerned with ease of use and perceived usefulness and did not include trust as an element, subsequent authors have expanded the model to include trust as an element (Gefen et al, 2003; Pavlou, 2003; Pikkarainen et al, 2004)

While trust and confidence in data security appear to be the primary factors inhibiting take up of cloud services, Shin et al (2014) argue that end users are more concerned with price, capacity and stability when assessing cloud providers than with issues of data security.

Some commercial research suggests a lack of confidence in cloud security among businesses (NTT Communications cited in Ashford, 2014), with up to 90% reconsidering adoption or changing procurement policies because of privacy concerns, while Sahandi et al (2012) found that 54.6% of SMEs would not consider cloud platforms because of data security concerns.

Research Philosophy

The way in which data is collected and analyzed is informed by the philosophy underpinning the research (Holden and Lynch, 2004). The predominant philosophical research positions are positivism and interpretivism (Hudson and Ozanne, 1988) although this dichotomy is sometimes challenged by a pragmatist stance (Goulding, 1999), and the duality often criticized as simplistic (Newman and Benz, 1998; Silverman, 1998).

The positivist approach assumes that all things are measurable, and can be subject to statistical analysis, contrasting with the interpretivist approach which holds that data is subjective and reality constructed (O’Donoghue, 2007). The positivist approach is the more popular approach among those seeking to understand consumer behaviour and attitudes (Hunt, 1991), which is what this paper ultimately seeks to achieve.
RESEARCH METHOD

In establishing a positivist philosophical approach, the selection of a quantitative research method derives logically from this position (Balnaves and Caputi, 2001). Quantitative research, at its most basic level, seeks to understand a phenomenon through the use of numerical data (Reaves, 1992) and this paper seeks to use statistical means to gain empirical knowledge about the attitudes of end-users to data security in cloud computing platforms.

DATA COLLECTION METHOD

The data was collected using a web-administered survey instrument. Web-based surveys are now considered a valuable research tool (Stelle, 2008), despite early concerns relating to validity (Krantz and Dalal, 2000; Braithwaite et al, 2003), mainly relating to the difficulty in finding representative samples among Internet users in the days before Internet usage became ubiquitous. The well documented advantages of conducting online surveys in terms of cost, and speed and ease of analysis (Wright, 2005), tend to outweigh the concerns regarding validity, which at any rate are less relevant today. The fact that the research was conducted among users of cloud computing platforms meant concerns about representation were less important.

SAMPLE SIZE

It is generally thought that low sample sizes in survey research have a negative effect on validity and statistical significance (Charter, 1999; Goodhue et al, 2006), although this is disputed by some (Wilkerson and Olson, 1997; Lantz, 2013).

The most common formula for the determination of an appropriate sample size is expressed thus-

\[ n = \frac{Z^2 \cdot p \cdot (1-p)}{\epsilon^2} \]

Where the Z value represents the confidence level and C the confidence interval or the acceptable margin of error (Bartlett II et al, 2001). In applying this formula with a commonly used confidence level of 95%, and using a confidence interval of +/- 5, a sample size of 384 would be required, while increasing the margin of error to +/- 10 would require a sample size of 96. This research was conducted on a convenience sample of 30 respondents and as such the maximum confidence interval at a confidence level of 95% is a very wide +/- 23.

Questionnaire Design and Relationship to Previous Research


While Burda and Teuteberg measured eight items, this questionnaire borrowed only four constructs - intention to use, risk, trust and reputation. While Burda and Teuteberg sought to construct a technology acceptance model for cloud computing, this research aimed to measure trust and the related concepts of perceived risk and supplier reputation, while also measuring what influence these concepts might have on intention to use. The questionnaire therefore sought to measure the four constructs using the same statements as Burda and Teuteberg, which are presented below. It is hoped that by replicating the research undertaken by Burda and Teuteberg, this research can add to the existing literature and build upon previous research in this area.
C1: Intention To Use
I would use cloud storage to archive my personal data
I am very likely to archive my personal data using cloud storage
I intend to use cloud storage for personal archiving in the future

C2: Risk
There is a high potential for loss involved in using a cloud provider for personal archiving
There is a considerable risk involved in using cloud storage for personal archiving
A decision to use cloud storage for personal archiving is risky

C3: Trust
Overall, my cloud storage provider is trustworthy
My cloud storage provider wants to be known as one who keeps promises and commitments
I trust my cloud storage provider keeps my best interests in mind
Even if not monitored, I’d trust my cloud storage provider to do the right job

C4: Reputation
My cloud storage provider is known to be dependable
My cloud storage provider has a good reputation in the market
My cloud storage provider has a reputation for dependability
My cloud storage provider has a poor reputation in the market

FINDINGS AND ANALYSIS

In total the survey had thirty responses. Of these, 50% were male and 50% were female. The age of the respondents was distributed thus:

<table>
<thead>
<tr>
<th>Age</th>
<th>Number of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>18-24</td>
<td>15</td>
</tr>
</tbody>
</table>

The results of the study are firstly discussed descriptively. The two hypotheses (H1 and H2) are subjected to statistical hypothesis testing in order to prove or disprove the null hypotheses. The two research questions (R1 and R2) are answered by way of measuring the strength of the correlation between the distinct constructs under measurement. The four tables below (C1, C2, C3, and C4) display the results of the survey instrument.
DESCRIPTIVE OVERVIEW OF RESULTS

INTENTION TO USE

Just over half the sample indicated that they would use a cloud platform to store personal data, although just 33.4% indicated that they would be very likely to do so, while 46.6% indicated that they intended to use a cloud platform to store data and some point in the future.

RISK

More than half of the respondents (53.3%) believed there was a high potential for data loss when using a cloud platform, while 66.7% believed that there was a considerable risk associated with using a cloud platform for data storage. A majority of respondents (56.6%) believed the decision to use a cloud platform for personal data storage was risky.

TRUST

46% of respondents believed their cloud storage provider to be trustworthy, and just over half believed their provider wanted to be seen as trustworthy. 40% of respondents believed that their provider had their best interests in mind, while just over 40% said they would trust their provider to do the right thing with monitoring.

REPUTATION

A majority of respondents (51.7%) believed their cloud provider was dependable, while 63.4% believed they had a good reputation in the market. A majority (53.3%) believed their provider had a good reputation for dependability, while a majority disagreed with the statement that their providers’ reputation was poor.

RESEARCH QUESTIONS AND HYPOTHESES

H1: Users of cloud computing platforms exhibit trust in cloud platform providers.

In order to test this hypothesis, the analysis used a one-sample t-test with a view to proving or disproving the null hypothesis. In this form of analysis, a t-value of less than 2.015 at a standard significance level of 0.05 would indicate that a majority of respondents disagreed with the statement, thus proving the null hypothesis. At a t-value of greater than 2.015, the alternative hypothesis is proven, indicating that the majority of the sample responded positively to the statement in the survey instrument (Wilcox, 2012).

As per the above table, the null hypothesis was disproved for all but one of the survey statements (my cloud storage provider wants to be known as one who keeps promises and commitments), suggesting either a lack of trust or an ambiguity among the sample respondents.
**H 2: Users of cloud computing platforms perceive the use of cloud computing platforms to be risky.**

In order to test this hypothesis, a one-sample t-test was again employed, as above. The results are displayed below:

<table>
<thead>
<tr>
<th>Mean</th>
<th>Mean %</th>
<th>SD</th>
<th>P value</th>
<th>T value</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.4</td>
<td>26.7</td>
<td>1</td>
<td>0.0366</td>
<td>2.1909</td>
</tr>
<tr>
<td>3.7</td>
<td>20</td>
<td>0.91</td>
<td>0.0002</td>
<td>4.2133</td>
</tr>
<tr>
<td>3.4</td>
<td>13.3</td>
<td>0.97</td>
<td>0.0316</td>
<td>2.2586</td>
</tr>
</tbody>
</table>

As per the table above, the alternative hypothesis was carried for all the survey statements within the risk construct, suggesting that the sample perceived that the use of cloud platforms for data storage posed a risk.

**R 1: Does provider reputation influence trust?**

The following table is the results of a correlation coefficient calculation between the survey items in constructs C 3 (trust) and C 4 (reputation), in order to answer R 1 and establish a relationship between trust and provider reputation. The strength of the correlation was calculated using Pearson’s (1896) formula, expressed thus:

\[ r = \frac{\sum (x - \bar{x})(y - \bar{y})}{\sqrt{\sum (x - \bar{x})^2 \sum (y - \bar{y})^2}} \]

<table>
<thead>
<tr>
<th>C3 (Trust)</th>
<th>C4 (Reputation)</th>
<th>R Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0.88</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0.87</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0.91</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>0.2</td>
</tr>
</tbody>
</table>

In this table, the survey item C3.1 (Overall, my cloud storage provider is trustworthy) displayed a high level of correlation (0.88) to the survey item C4.1 (My cloud storage provider is known to be dependable). The survey item C3.2 (My cloud storage provider wants to be known as one who keeps promises and commitments) displayed a high level of correlation with C4.2 (My cloud storage provider has a good reputation in the market). The survey item C3.3 (I trust my cloud storage provider keeps my best interests in mind) displayed a high level of correlation with the survey item C4.3 (My cloud storage provider has a reputation for dependability). The survey item C3.4 (Even if not monitored, I’d trust my cloud storage provider to do the right job) displayed a low correlation with the negative statement contained in the survey item C4.4 (My cloud storage provider has a poor reputation in the market).

The findings therefore show, at the very least, a correlation between positive expressions of trust and positive statements about supplier reputation, echoing the results achieved by Burda and Teuteberg.

**R 2: Does perceived risk influence intention to use cloud computing platforms?**

The following table is the results of a correlation coefficient calculation between the survey items in constructs C 1 (Intention to use) and C 2 (risk), in order to answer R 2 and establish a relationship between intention to use and perceived risk.

<table>
<thead>
<tr>
<th>C1 (Intention to Use)</th>
<th>C2 (Risk)</th>
<th>R</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0.56</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0.27</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0.75</td>
</tr>
</tbody>
</table>

In this table, survey item C1.1 (I would use cloud storage to archive my personal data) displayed a relatively high correlation with C2.1 (There is a high potential for loss involved in using a cloud provider for personal archiving), although this was not as high as the correlation between trust and provider reputation across any of the survey items. The survey item C1.2 (I am very likely to archive my personal data using cloud storage) displayed a low level of correlation with survey item C2.2 (There is a considerable risk involved in using cloud storage for
personal archiving). The survey item C1.3 (I intend to use cloud storage for personal archiving in the future) displayed a high level of correlation with survey item C2.3 (A decision to use cloud storage for personal archiving is risky).

The relatively low correlation between C1.1 and C2.1, and the low correlation between C1.1 and C2.2 might indicate that end-users are willing to use cloud services despite being aware of the risk to data loss. As previously, this may be because casual users of cloud computing services store less sensitive data than business users, and also because they do not have to conform to a regulatory data protection security framework in the same way as business and enterprise users (Carey, 2009). Among younger users, it is also possible that they lack an expectation of privacy as they are accustomed to making data available on social media sites (Marwick and Boyd, 2014).

The Findings in the Context of Previous Research

Taking perceived risk as analogous to satisfaction with cloud security, this sample was less inclined to associate cloud platforms with data loss as were the business users surveyed by Alijani (2014). This could be that business users were conscious of having more to lose than domestic users, or simply that they were more aware of specific technical threats to data security in the cloud. The number of respondents, who replied positively to statements about risk and trust, was higher than the SMEs studied by Sahandi et al (2012), the majority of whom would not consider using cloud services because of security concerns. As before, this might point to a lack of awareness about security issues among casual users of cloud services.

Limitations of this Research

The primary limitation of this research was the low sample size, and the associated presumed negative effect on validity and the inherent difficulty in drawing an inference to the population at large.

The respondents were casual users of cloud storage platforms, so comparisons with previous research into business and enterprises users, while providing an interesting context, are of lesser value as a whole.

A more specific survey instrument, which sought to gain insight into attitudes towards particular cloud storage providers, might have provided a stronger basis for future research while offering a valuable insight to industry.

It is also worth noting that the application of Pearson’s formula to the constructs in R1 and R2 merely measures the strength of correlation. While it is possible to infer probabilistic causation from strong correlation (Dempster, 1990), conventional wisdom would suggest that correlation does not imply causation (Jacobs et al, 2007).

Conclusions and Recommendations

In line with previous work on the subject, this research identified a perception among users of cloud computing platforms that storing data in cloud platforms entails a degree of risk. This is despite improvements to data security procedures and the development of new technologies designed to make data storage in the cloud more secure. It is incumbent on cloud platform providers to educate users about these advances in data-security technology, perhaps by making security part of their marketing and differentiation strategies, if they wish to drive take-up of services and reassure customers about data security.

The study also revealed a lack of trust, or an ambiguity towards statements measuring the trust construct among the survey sample. Payne’s (2013) recommendation that providers should work to build trust through increased transparency seems to hold relevance among this sample, and the assertion by King and Raja (2010) that building poses a major challenge for the cloud computing industry still hold true some five years later, in spite of technological improvements to data security issues.

A significant correlation between the trust and reputation variables suggests that building and maintaining a strong reputation for security and
reliability can go some way to towards overcoming issues around trust among end users, and it follows therefore that, in addition to educating users about improved security technology, cloud platform providers should manage their reputations in the marketplace to increase end user trust in the security and reliability of their platforms.

REFERENCES


69. Payne, S (2013) Building Trust Between Cloud Providers and Consumers. CIO, 3rd April, p. 6


