Trouble in the cloud leaves businesses tied to their servers

May 16 2014, by Shehnila Zardari

The cloud is on the horizon but not fully attainable. Credit: Greg McMullin, CC BY-NC-ND

Cloud computing is being heralded as the next big thing. Gone are the days when people and businesses need to maintain expensive hardware to store their information, they can now pay someone else to look after it and access it whenever or wherever they like. But problems with the way the cloud operates are holding us back. Users are not quite ready to move completely to this brave new world because of some potentially serious glitches.

One particularly exciting feature of the cloud is the cost of using it. You spend money on storing information on someone else's server rather than maintaining your own.

But the cloud has a significant caveat. It is essentially a black box. Users know little about its internal structure, how it functions and who has access to the data inside. We put information up there and hope it comes out again, without knowing anything about what happens in between.

Amazon Web Services, one of the biggest providers in the world, has tried to win the confidence of users by publishing information about its security mechanisms. But a look at this information reveals that, due to the unpredictable nature of the internet, the company cannot guarantee the security of user data. The users are therefore responsible for protecting and backing up their content.

Careful reading of Amazon Web Services' customer agreement shows that the company is not liable if your data is altered or deleted, nor if it is affected by any kind of security breach. The only thing the company promises in the service agreement is that the cloud will be available 99.95% of the time. If it isn't, the customer gets compensation in the form of credit.

That means if the customer has paid upfront for using the cloud for ten hours, they are tied to the contract, even if the uptime was below 99.95%. All they get if the service was down is more time in the cloud. They don't even get a refund.

This is a significant problem that could put customers off. If a business has stored large amounts of data in a cloud service and there is a fault, the cost of the downtime – even if it is very short – may be significant. It might even be more than the investment made in using the cloud service in the first place.

Getting locked into the wrong cloud in this way is a major concern for users and prevents them from adopting the new service. Due to the non-negotiable nature of service agreements, users have little recourse if things go wrong. The cloud service provider is always in a win-win situation.

We identified a number of other risks that cloud users might come across. These included the potential for insiders with malicious intent to access their data; difficulty accessing the data for other reasons; and the need to comply with certain standard set by the industry.

Problems like these could lead to financial losses, a loss of customer trust, damage to business reputation, losing company secrets and even the risk of going bust. The risks are huge and cannot be ignored.

Silver lining

Most of these problems can be solved though, and the solution lies in the agreements users make with cloud providers.

A university, for example, is subject to the freedom of information act in the UK. That means it has certain obligations relating to how it handles data. A university cannot afford to send its data to any cloud whose data centres are based outside the European Union because of the Data Protection Act 1998. Those servers may be based in a country that does not have the same regulations as the UK so the data may not be as secure.

Similar problems are faced by health authorities that need to store sensitive information about patients. Even organisations who store less sensitive information may have to deal with completely unanticipated problems if they store their information on servers in far away places.

For these reasons and more, a cloud service provider must inform potential customers if they send data to centres in other countries. For UK universities, this means stating if the centre is based outside the EU. The terms of service are the ideal place to raise this.

Since the cloud is a black box, customers have to rely on the information given to them in the terms of service to make decisions about whether to use the cloud. They also need to rely on the reputation of providers to decide which service to choose. This is of utmost importance because they are, in many respects, handing over the governance of their data to a private company.

At the moment, the terms of service offered by cloud providers are far too static. To make the adoption process work, it is important that they negotiate their terms of service with users according to their requirements.

Different organisations have different needs and that will have to be reflected in terms of service if our future really rests in the cloud. As well as stating where servers are, individual contracts should also be able to provide clear information to customers on any other factors that might undermine their commitments to local legislation.

Businesses want to use the cloud. It is a cost effective way to store the immense amount of data being created these days. But they are wary because of the risks still inherent in cloud adoption. Significant creases need to be ironed out before they can safely ditch their servers.

This story is published courtesy of The Conversation *(under Creative*

Commons-Attribution/No derivatives).

Provided by The Conversation

Citation: Trouble in the cloud leaves businesses tied to their servers (2014, May 16) retrieved 23 April 2024 from https://phys.org/news/2014-05-cloud-businesses-tied-servers.html