Cloud Computing: The Emperor's New Clothes of IT

Henry B. Wolfe
University of Otago, Dunedin, New Zealand

hwolfe@infoscience.otago.ac.nz

Abstract

Cloud computing has recently become a hot topic in IT circles. Organizations see it as an opportunity to reduce costs. Outsourcing the provision of data services has become an attractive option in the current climate promising the reduction of staff, equipment, IT operations and associated costs. This paper makes the case against using cloud computing for anything but the most trivial IT requirements. The issue is jurisdiction and what happens to your data when things go wrong. Contracting plays a big part in the process and most cloud computing contracts absolve the service provider of any responsibility for security, continuity of service, or for the integrity or privacy of the users' data. There can also be issues surrounding access to a user's data by official and unofficial entities. Data, such as client lists, proprietary information, and other sensitive information is the organization's most valuable asset and should never be managed or controlled by any outside entity.

Keywords: cloud, jurisdiction, contract, privacy.

Introduction

Cloud computing provides shared resources, software and information available on demand over the Internet enabling organizations to avoid the cost of owning and managing their own IT facilities and staff. It may also provide the availability of raw processing power as well. In reality, the user stores their information on servers located at a giant data center somewhere – the cloud and is able to process and/or retrieve that data using a Cloud Client.

This service enables organizations to reduce the need for IT staff, equipment and facilities. It would seem that there are significant savings to be made by moving to cloud computing. However, savings are only one part of the equation. What also must be considered is the protection and control of organizational data and the continuity of service provided. There are often statutory requirements that influence the control and storage of specific information – such as payroll and tax records. The nature of this kind of information has privacy implications as well. Organizations also have other strategic and proprietary information that it deals with such as client data. This information is the life's blood of the organization. Placing it under the control of a cloud service provider who may have a different agenda may not be in the organization's best interest.

The idea of shared resources is not new. Time sharing may be compared to cloud computing (the early days of computing in the mid to late 1960s). You knew where your data was physically housed and who had access to it. The timeshare provider was usually in the same building, town or state/province and was therefore bound by the laws of the jurisdiction where the users resided. Remote hackers did not present the risk they do today. Time sharing provided internal processing, storage of data, and other services to users who did not have to absorb all of the costs associated with owning and operating a computing center. Competition for those resources was often problematic. Data passed either directly over a cable or over the telephone system through a modem. This data was not normally accessible by unauthorized users and therefore reasonably secure from external attack. When PCs became able to process business data, control shifted back to the user. Computer networks since then have been used mainly for communication and data transfer between users and between entities.

You can outsource responsibility but you can't outsource accountability (Reed, 2010). The cloud paradigm centralizes IT control with the service provider. One of the problems is that the service provider may not be in the same jurisdiction as the user. This has the potential to cause problems and raise unacceptable risks. A survey was mounted by the Cloud Legal Project at the Centre for Commercial Law Studies, within the School of Law at Queen Mary, University of London. The survey examined Cloud Computing service providers' terms and conditions. One of the key findings was that most providers assert "wide-ranging disclaimers of liability or any warranty that the service will operate as described" (Bradshaw, Millard, & Walden, 2010). This is an important issue since a client is expected to entrust all of its most sensitive information and data to an organization that purposely takes no responsibility for that trust. This doesn't make any sense within the realm of risk analysis or good business practice. At the end of the day, management and directors are responsible and accountable to stakeholders for their decisions and how they impact business success or failure.

Cloud Computing Issues

Cloud computing has many issues that must be addressed before any decision can be made to contract such services. When contemplating outsourcing, the issue of *what happens if it all goes wrong* must be considered. In any given IT installation time and resources will have been expended to document and prepare a plan that will ensure recovery in the event of a disaster (a continuity or disaster recovery plan). Two of the principal areas of concern are the legal and jurisdictional issues surrounding any given cloud service provider. The following is a preliminary/partial list of cloud computing issues:

RISK Issues

Who owns the risk? (owner or provider)

Risk ownership is important. After outsourcing IT services to the cloud somewhere the risks associated with that activity will devolve to one or the other. Every organization is accountable to their stakeholders and risk is an integral part of that accountability. The owner of the risk is responsible for mitigating that risk. If the owner has that responsibility, how will it be able to satisfactorily provide mitigation without controlling the IT process? In cloud computing, the client/owner does not control the cloud IT function and therefore does not control the security in place yet when things go wrong the owner will be held responsible. If a Sarbanes-Oxley Act, which holds directors responsible for all aspects of the business including IT and its security (Sarbanes-Oxley, 2002) or other similar legislation is in place in the owner's jurisdiction, then this issue will be of particular importance to the organization.

Who can access your data?

This depends on the cloud service provider and whether there are specific clauses regarding access within the contract. The prospective client must decide who exactly they wish to have access to their data and at what level. That should be formalized in the contract or service level agreement. *FaceBook*, while not cloud computing, is a good example of a social service provider using data mining techniques to profit on what some people perceive as private information (The Telegraph, 2009).

RISK/AUDIT Issues

Who is responsible for information security?

Most service providers, including cloud service providers, try to absolve themselves of any responsibility and will expect that the client be responsible for information security. This may in part be accomplished by only storing strongly encrypted data in the cloud. However, that does not protect against an entirely different kind of attack such as a distributed denial of service attack from the Internet vector where continuity is compromised. Security against that kind of attack is squarely in the control of the service provider. This is another reason why the service provider must be independently audited - regularly.

What is acceptable use? Can the cloud service provider mine your data? Facebook, though not cloud computing, is a good example of mining people's personal data for a profit.

If acceptable use is not clearly and concisely defined contractually, then it is likely that the service provider will mine client data as well and client activity and make whatever use is necessary to make a profit from it. This must be contractually and formally defined prior to engaging a cloud service provider.

CONTRACT/AUDIT Issues

Who validates the security provided by the cloud service provider?

Will the cloud service provider allow a security audit on their facilities? Who will they allow do this important function? Will they require that their auditors or affiliate auditors be used? What validity would be placed on an internal audit? This problem raises more questions than answers. Without a valid and independent security audit of cloud computing services, a client cannot be assured or confident that proper security measures and procedures are in place.

What happens to your data when the cloud service provider becomes subject to a forensics investigation?

Such investigations may be totally unrelated to the client and service provider but rather focused on another client. In any case, forensics investigators can capture all data on any given device. That may mean that client data is captured because it resides on a server where the targeted suspect also has its data stored. Once again such an event needs to be clearly defined and concisely described in the contract mitigating the risk to the innocent client to their satisfaction.

Will you have the right to audit the cloud provider's procedures and security?

This is unlikely unless the client succinctly specifies that requirement in their contract. The service provider may not allow any independent audit. If that is the case, it may be time to look for a different service provider.

How do you ensure that your data is fully segregated and not co-mingled or accessible by others?

The only way is to do so is contractually, however, there would also be a need to periodically audit the service providers facility to ensure that segregation is in fact in place. The reason for this segregation is to reduce any risk that two or more clients' data is not inadvertently made available because of it being co-mingled.

How do you prevent cloud administrators from seeing or copying your data?

Administrators have no business browsing any client's data. The simple fact is – you can not stop them. Some administrators will have full access to everything on the systems they are responsible for. It may be important to require full disclosure regarding the provider's policy on hiring and background checks. This could perhaps allay some concerns of the client but it is not foolproof.

How will you know that all web vulnerabilities have been addressed and properly managed on an ongoing basis?

Unless you have an independent auditor/penetration tester analyze the service provider's facility for vulnerabilities and weaknesses, you will not know. Independent audits must be done periodically because the threats and vulnerabilities change continually. Service providers are reluctant to allow these audits/tests.

Will all of your data be encrypted with "strong" encryption? Who implements and controls the encryption?

Strong encryption (for an explanation see *Strong Encryption* the definition in the *Glossary*) is used to protect the integrity and privacy of sensitive data. In a proper system using such a technique, only authorized persons will possess the specific encryption/decryption algorithm and keys. If you specify that all or specific parts of your data is encrypted with strong encryption, what audit controls are in place to ensure that the strong encryption has not been compromised and is used in the correct way with only the client knowing the keys. In some jurisdictions, encryption keys must be made available to various government agencies. Is that an acceptable situation?

> **A personal note**: Privacy is a human right not a privilege granted arbitrarily by some government. On the 10th of December 1948 the *General Assembly of the United Nations* adopted and proclaimed the *Universal Declaration of Human Rights*. *Article 12* states "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" (United Nations, 1948). Strong encryption enables everyone to control and protect this very important and most basic of

human rights. Do you really want your data and information stored in a jurisdiction where this human right has been abrogated?

Cloud computing contracts are not designed to protect the client. Many have clauses that will significantly impact - negatively - the client.

After studying thirty-one cloud computing service providers' terms and conditions, the evidence speaks clearly and loudly that cloud service providers generally assert "*wide ranging disclaimers of liability or of any warranty that the service will operate as described, or indeed at all*". (Bradshaw et al, 2010)

The provider will generate information about the client during the course of providing the service. What information will be generated and what will be done with it?

Privacy of information is a serious issue as discussed in #11 above. What guarantees that can be proven and that are auditable does the provider offer to protect the privacy of the client and any activity carried out in the cloud by the client? Activity information has a value and can be exploited. One must always remember that the service provider is a business like any other whose primary interest is making a profit. Selling this type of information provides an attractive revenue stream with little associated cost.

Dispute resolution: is the mechanism formalized – in most cases it is not.

Dispute resolution including procedures and the specific jurisdiction wherein any given dispute between client and provider should arise must be contractually formalized. If that is not the case when there are clearly choices, then the cloud provider will choose a jurisdiction which will be more favorable to their position. To ignore this probability would be to ignore the potential associated risk. It is far better to have protective measures in place and not need them than to need them and not have them available.

What is the reaction from users' customers when they find out that their information is now or will potentially be stored in a cloud computing environment?

Unless the cloud user informs their customers, it will be assumed by the customers that their information is located in the user's jurisdiction giving a sense of confidence to the customer that any problems can be resolved there. When it all goes wrong it would be reasonable to consider that the organization's customers may well be at risk.

Service Level Agreement/ CONTRACT Issues

What kind of incident response system does the cloud provider have in place? How and when is the client informed of such an incident?

If the cloud provider is successfully attacked how will the client be notified of the event? What exact procedures are taken when an event occurs and what happens if client data is compromised,

revealed or destroyed? Clients who would use cloud computing will be depending on the continuity of the service as well as the service provider's ability to protect clients' data from access, corruption, modification, or theft. The client will also be depending on the service provider to provide a quick and complete recovery so that service is not interrupted for any longer than necessary.

The IT function is no longer an option in the vast majority of organizations. It is vital to the continued operation of most organizations and potential revenue streams for many. Service interruptions have a cost. It they are protracted, the probability raises that the organization's ability to continue to function may cease. Therefore, continuity must be addressed in the Service Level Agreement with penalty or indemnification clauses providing protection against potential consequences of such occurances.

How do you ensure that all copies of your data are properly and adequately destroyed?

Is there a documented and verified procedure for destroying data? Merely deleting data does NOT remove it from the server's hard drive(s) - (for an explanation see the *Data Deletion* explanation in the *Glossary)*. When the client either wants particular data destroyed (over written) or when the client severs the contractual relationship with the cloud provider, procedures that are documented, verified and audited must be in place to ensure that all or specified client data is completely overwritten wherever is may be stored – including in all backups and archives of the service provider. If strong encryption is used then if client data were to resurface at a later time that risk would be mitigated.

Ownership rights emanating from the cloud computing relationship.

As a result of activities between the user and provider, information of various types will be generated. Ownership of that information can become an important issue. For example, the amount of usage and traffic patterns information can be generated by the provider with the innocent and justifiable reason that the information is needed to manage the cloud resources and performance on offer. On the other hand, this information has a market and could be useful to the user's competition. Use of this type of information should be clearly defined within the contract.

The bigger the target, the more attractive it (any given cloud provider) will be to the hacking community.

The nature of cloud computing is to centralize the storage of very valuable data in a single place. That fact makes targeting a cloud provider a challenging and high value target. If hackers are successful in an attack against a cloud provider, not only is that provider hacked but everyone who is served by that provider may also be hacked and their data and information exposed or compromised. Therefore, cloud security becomes even more important to prospective clients.

For example in other aspects of computer security we have seen, Microsoft as the biggest organization of its type being attacked repetitively. If a hacker was able to find an exploit for just one of Microsoft's products, it would open a huge community of users of that product to being attacked. To attack lesser known and less prolific software vendors' products is less like to pay off in the same way.

JURISDICTIONAL Issues

Which jurisdiction's rules and laws apply when there is a legal dispute? (owner or provider)

The answer to this question may make the difference between obtaining justice in a dispute and having essentially no recourse. Jurisdiction usually plays a key role in dispute resolution. Users would be wise not to engage or contract a cloud service provider that does not locate its entire operation within the same jurisdiction and client. If the provider is an international corporation, it is very likely that they will have server farms in different jurisdictions. Unless otherwise contracted, in the event of a dispute the provider will select the jurisdiction which will be most favorable to its position.

Who is legally responsible? (owner or provider)

That will depend on the jurisdictions where the two parties reside and which prevails. If it is not contractually agreed, then it is likely that there will be an additional dispute about jurisdiction when issues arise. This is another place for conflict.

What happens to your data when the cloud service provider shuts down, goes bankrupt, or is bought up by another organization?

The answer to this question will depend on jurisdiction. If the jurisdiction is not favorably disposed to privacy matters or if there is no built in protection of data held in the cloud the outcome could be unpredictable. In business, certainty is paramount. If a client's data becomes freely available in an unrestricted jurisdiction the client organization will be damaged. To what extent will depend on the kind and sensitivity of information held by the cloud service provider on the client's behalf. Organizations contemplating involvement with cloud service providers should negotiate and contractually formalize the specifics for each of the three possibilities identified.

Whose privacy laws prevail? (owner or provider)

Once again, jurisdiction will prevail. Selection of a cloud service provider may or may not entirely clarify this risk. Some cloud service providers have server farms in more than one jurisdiction (see #20 above).

In various countries, law enforcement can bug internal traffic under Internet surveillance legislation. How will your data be protected against this?

In the event that the client wants to maintain it privacy and protect its traffic from unauthorized eavesdropping or unwanted surveillance, how will it be handled by the provider? In some jurisdictions it may be unlawful to deprive law enforcement or intelligence from being able to view all communications traffic. How will the clients' best interest be served if the provider cannot or will not protect clients traffic regardless of the reasons/excuses put forward? Organizations who are concerned about the privacy of their activities may well consider contracting a cloud service provider that is located in a jurisdiction where surveillance and interception activity is not a part of national policy.

An Example

The US Department of Homeland Security (DHS) intends to deploy *Einstein 3*, a surveillance system under the cover of "intrusion prevention technology". However in the process this system makes use of deep packet inspection (see the explanation in the *Glossary*). The content of every packet that passes over Government servers will be analyzed, in real time, and actions taken depending on what has been discovered. This issue is also currently being addressed by the European Commission in an action against the UK. Their concern is that unlawful interception in the UK constitutes a breach of EU Privacy Law (Directives *2002/58/EC* and *95/46/EC*). These issues further justify the use of strong encryption to protect every person's human right to privacy – especially regarding the payload packets of every message. The technology used by *Einstein 3* (deep packet inspection) is not exclusive to this system. According to EPIC (Electronic Privacy Information Center) DPI has been used in attempts to: "build profiles of consumers for marketing purposes; intercept communications at the request of law enforcement (both with and without warrants); enforce copyright laws; prioritize the transmission of some packets over others; and identify computer viruses and spam." (EPIC, 2011)

A Potential Solution

If an organization chooses to make use of cloud computing, it may be possible to reduce some of the risk in two ways:

1) The first is by detailed contract negotiation wherein the issues discussed above (and others of import) are addressed specifically and formally and agreed to by the parties - to the satisfaction of the user organization.
2) The second adds an additional measure of protection. By simply encrypting all data stored in the cloud using strong encryption at the user end **only** the organization can ensure that data will not be compromised. Further, the user organization must not make the algorithm or the keys used to encrypt and/or decrypt available outside the organization. If the cloud service provider demands any of those on behalf of itself or because it is required to by virtue of the jurisdiction then you might just as well not encrypt or select a different cloud service provider that meets **your** terms.

Summary

Outsourcing has over time shown great opportunity for saving money. However, there is more to outsourcing than saving a few bucks here and there. As can plainly be seen from the long and by no means complete list of issues outlined here, outsourcing IT into some cloud – somewhere has many pitfalls. This is especially true because the IT function is critically vital to almost every organization. The one thing that we should all know is that eventually things will go wrong. The timing of such events is actually and practically not predictable but when it does happen we must be ready. It would be incompetent of management not to address these risks and plan for the worst. Due diligence is what we do to minimize risk. The elements of the various risks outlined in this paper are but few of the more important issues that must be dealt with decisively before contracting any but the most trivial applications into the cloud.

Glossary

Data Deletion: Erasing or deleting a file on any give hard drive consists of the operating system changing the first character of the file name in the file allocation table to a hexadecimal "***e5***".

That code tells the computer's operating system that the space allocated to that file is now available for reuse (once a file has been deleted it is also known as unallocated space). The data that occupied the clusters (the discrete addressable space) on the hard drive before the erase or delete command was executed continues to reside in those same clusters until such time as the operating system needs to store a new or updated file. It may then overwrite that unallocated space with the new data. The timing of this event, however, is unpredictable and therefore a deleted file may be overwritten instantly or remain on the drive indefinitely.

Deep Packet Inspection (DPI): Inspection and analysis of packet content based on some predefined strategy. "Deep Packet Inspection (and filtering) enables advanced network management, user service, and security functions as well as internet data mining, eavesdropping, and censorship." (Wikipedia, 2011) This occurs in real-time. In the case of Einstein 3, that strategy could be identifying malware or intruder attack signatures and it could also be the identification of key words, key phrases, or key concepts or ideas as defined by DHS. The claim is that this system will only be used on Government systems. Any way you look at it, it is an invasion of the privacy of every user whose data passes through servers that make use of the DPI technique (which is not exclusive to DHS) and those controlled by DHS or its agents (those who would cooperate either by choice or by force).

Strong Encryption: Is an encryption method that has been vetted by the cryptographic community and found to be without any flaws that could be exploited. Once this attribute is proven, then the size of the keys define the key space and how long it would take to derive the keys for any given message by the use of a brute force attack. A brute force attack tests each key for that entire key space – one at a time. The size of the key space can make encryption strong if the time necessary to carry out a brute force attack will not produce a result in a useful timeframe. For example: the **I**nternational **D**ata **E**ncryption **A**lgorithm (IDEA) has been in the public arena for twenty years having been repeatedly analyzed and tested. It is considered to be a strong encryption algorithm and it has a key space of 2^{128} – that equates to the number 340 with 36 zeros after it – or more than all of the atoms in the known universe. No computer in existence today or considered possible in the foreseeable future could step through that number of keys in anything less than millions of years.

References

Bradshaw, S., Millard, C., & Walden, I. (2010). *Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services.* Legal Studies Research Paper No. 63/2010, Queen Mary University of London (School of Law), September 2010, http://ssrn.com/abstract=1662374

Department of Homeland Security, Einstein 3. (2010). *Privacy impact assessment for the initiative three exercise.* Retrieved from http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3exercise.pdf

EPIC (Electronic Privacy Information Center). (2011). *Deep Packet Inspection and Privacy*. Retrieved from http://epic.org/privacy/dpi/

Reed, C. (2010). *Information "ownership" in the cloud.* Legal Studies Research Paper No. 45/2010, Queen Mary University of London (School of Law), September 2010, http://ssrn.com/abstract=1562461

Sarbanes-Oxley. (2002). *Public Law 107-204* -- July 30, 2002, enacted by the 107th Congress of the US, http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html

The Telegraph. (2009). N*etworking site cashes in on friends.* Retrieved from http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/4413483

United Nations. (1948). *Universal declaration of human rights.* Retrieved from http://www.un.org/en/documents/udhr/index.shtml

Whitmore, P. (2010). *Security among the clouds.* Price Waterhouse Coopers International Limited. Presentation at the BrightStar Conference , 30 March 2010, Auckland.

Wikipedia. (2011). *Deep packet inspection*. Retrieved 28 February 2011 from http://en.wikipedia.org/wiki/Deep_packet_inspection

Biography

Dr. Wolfe has been an active computer professional for more than 50 years. In 1979 Dr. Wolfe took up an academic post at the University of Otago. Since 1984 he has specialized in computer security. During that period he has earned an international reputation in the field of electronic forensics, encryption, surveillance, privacy and computer virus defenses.

Dr. Wolfe writes about a wide range of security and privacy issues for *Computers & Security*, *Digital Investigation* (where he is also an Editorial Board Member), *Network Security*, the Cato Institute, *Cryptologia*, and the *Telecommunications Reports*. He is a Fellow of the New Zealand Computer Society. He is also a member of Standards New Zealand SC/603 committee on Security, a member of the New Zealand Law Society's Electronic Commerce Committee, and was on the Board of Directors of the *International Association of Cryptologic Research* finishing up in January 2003.