Spring 3-27-2012

Exploring security issues in cloud computing

Katie Wood
University of Wolverhampton, k.wood@wlv.ac.uk

Exploring security issues in cloud computing

K Wood
Department of Informatics
University of Wolverhampton, UK
K.Wood@wlv.ac.uk

Abstract
Cloud computing has promised to transform the ways in which we use and interact with information technology (IT). The claims of significant benefits for businesses by using cloud systems are being overshadowed with the increased concerns about security, particularly privacy. This paper explores the unresolved concerns that businesses and users are still facing in terms of ensuring their data remains secure within a cloud environment. Through illustrating these issues with recent security breaches, the evidence clearly suggests they are hindering cloud adoption. Unless more focus is placed on security then cloud platforms are unable achieve cost saving benefits, improved efficiency or performance for a business. This paper argues that rather than cloud computing reaching its potential there are still remaining issues that must be addressed.

Keywords: security; data loss; data protection; cloud service providers (CSP); misconfiguration; cloud legislation.

1. Introduction

Given the current economic challenges facing businesses, there is more pressure to operate more flexible and effectively in order to remain competitive. As society has become more reliant on technology in many different aspects it is essential that the most reliable systems are in operation. The development of cloud computing has promised to transform the ways in which we use and interact with information technology (IT). Cloud has brought new opportunities for users and businesses to exchange data and resources in a more efficient manner. Alongside these benefits there are also concerns with using this form of shared system, especially in regards to security and privacy. Unlike previous systems such as an external network which the business has complete control over the system and data storage, this is not the case with cloud. These responsibilities tend to be under the control of a Cloud Service Provider (CSP). Therefore additional security risks have emerged through placing trust in a CSP to protect your data as well as the lack of information that users are provided with especially in regards to security and date storage.

The main objective of this paper is to provide a security perspective on cloud computing and highlight the key security concerns that are associated with this form of distributed system. It is evident that these must be addressed in order to protect users and cloud service providers and restore trust between the two after several highly reported security attacks on clouds in recent years. It is no wonder that the future of cloud is uncertain. This paper argues that rather than cloud computing reaching its potential there are still remaining issues that must be addressed. Unless more focus is placed on security then cloud platforms cannot achieve cost saving benefits, improved efficiency or high performance for a business.

The rest of this paper is organized as follows: Section 2 defines cloud computing and highlights the different popular forms of cloud; Section 3 highlights the concerns that still remain over using cloud; Section 4 focuses on some of the important security issues related to cloud computing; Section 5 considers the user responsibility in securing their data and selecting the right cloud services to fit their requirements; Section 6 looks at possible ways to improve the situation in clouds; Section 6 highlights the further works of the author, mainly in developing a framework for PaaS to improve configuration processes; Finally, Section 7 summarizes this paper and discusses future work

2. Defining Cloud Computing

Cloud computing is still an evolving paradigm. It is the next step in 'on demand' information technology services. The first challenge that users experience with cloud computing is understanding what the term means. There is no' precise definition' [1] for cloud. This has lead to arguments by researchers that the term "cloud computing" is far too broad making it difficult to develop a single and clear definition. Currently, there are over 20 different definitions. The most regularly used definition is by the National Institute of Standards and Technology, referring to Cloud Computing as:

"A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources ... that can be rapidly provisioned and released with minimal management effort or service provider interaction." [2]

The aims of cloud are to quickly release and upgrade these resources to the end user with minimal management effort or service provider interaction. Therefore cloud promotes availability through a range of different service and deployment models.

Cloud technology is already used on a range of devices including laptops, desktops PCs, PDAs and most new generations of mobile phones. Cloud technology has been integrated in these as it provides users access to processing, storage and applications over the internet while on the move. Users can then obtain applications and data 'on demand', which potentially can reduce costs for each user as they no longer require an expensive IT infrastructure or the costs of maintaining and upgrading. Cloud services do not take up space or processing power on the user's devices. The user gains access to the resources through a web browser, with the resources stored on the providers servers. In essence, cloud computing is really just an extra-large data centre that can provide services and resources to businesses and individual users. These cloud networks have the ability to manage multiple infrastructures across multiple organizations consisting of frameworks providing mechanisms for self-healing, self-monitoring and automatic reconfiguration [2]. Therefore in theory cloud appears to be the answer to issues facing businesses in this difficult economic climate, however in practice it is not as straightforward.

2.1. Key Cloud Services/Models

There are three different service models currently available for users, each has their own unique characteristics and benefits to the user.

Software as a Service (SaaS). This model allows applications to run on a cloud infrastructure. The applications are accessible from various client devices (e.g, PDAs, desktops) through a web browser. The provider has full control and manages the underlying infrastructure which includes network, servers, operating systems, storage, and applications. In some cases users have control of some application configuration processors.

Platform as a Service (PaaS). Platform provider users have either full or partial application development environments via the internet. Users do not have control of managing the underlying cloud infrastructure. This includes control of the operating systems which IaaS users have some control over. PaaS does provide users with some control with regards to deployment onto the cloud and application hosting environment configurations. This form provides the user with full access online and allows collaboration.

Infrastructure as a Service (IaaS). Users gain a full computer infrastructure via the internet. Users are provided with some control in regards to deploying and running operating systems and applications on their devices, as well as some elements of the network to deploy their own security measures such as firewalls. Again, similar to SaaS users, they do not have any control of the underlying infrastructure.

2.2. **Deployement Models**

There are currently four popular deployment models by cloud services can be deployed. [3]

Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

3. **Concerns over Cloud Uptake**

In September 2011, [4] the Dutch Minister of security and justice informed the government of the concerns of using US Cloud Service Providers (CSP) as they could be compelled to share data with the US authorities due to the provisions of the Patriot Act. A detailed report by Dutch IDG news site Webwereld [5] confirmed that the Patriot Act could override data protection and privacy legislation. Data protection and privacy are critical in order to protect user's data and keep data confidential within a cloud. These concerns have recently been echoed by other European Parliaments [6] The US government has been criticized as using USA CSP businesses as a way to get into Europe. The fact the most popular cloud providers are US companies – Google, Amazon, and Microsoft, it is understandable that concerns are growing over how much power and access to data the US could have through clouds. Other countries, for example China and EU countries are realizing the consequences of another country been able to access their data and could result in their national security being comprised. This is a stumbling block for potential users opting to use cloud services. As a CSP is a hosting business they store the user's data in their data stores. Users are becoming increasingly concerned over using cloud systems to store personal and sensitive data, especially as they have no idea where their CSP has placed this data. The number of reports of data loss, due to security breaches is on the rise rather than decreasing, due to the increase number of different CSP and user requirement. Microsoft [7] Google [8] are two of the main CSP both have experienced several security breaches. This is leaving users wondering if cloud is really the way forward, especially in terms of security.

There are several risks associated with data protection when using cloud computing:

• Possible unauthorised access to your data
• Loss of control to a CSP
Loss of data by either the CSP or a third party involvement might occur
• Malicious activities that rapidly spread on the cloud – that business is powerless to control or prevent
• Employees are not trained or experienced in using cloud services therefore compromising data protection

Table 1: Data protection risks in cloud computing

Within the UK, businesses holding personal and sensitive data are required to comply with the Data Protection Act 1998 [9]. Traditionally, with systems which are in-house, the business can identify relatively quickly any concerns and possible breaches before data is compromised, as there are no clear laws or legislations over the level of protection CSP should provide. Therefore the level of protection differs between each CSP and the types of services offered. Through cloud, businesses lose control over their data and therefore have no real assurances the data will be fully protected to the level they require in order to operate within their environment and be protected against breeches. One issue is the response of CSP. Some are relatively hands-off and will take minimal responsibility of security, performance and reliability of the service. This can have serious implications to business and could result in data lost or failure to follow laws and regulations that they are required too.

This raises the question; can you trust a cloud service provider? The fact that users of cloud services are often not informed that their personal information has been given to a third party or security breach has occurred creates doubt. This means that their data can be compromised and they are not informed of the full extent of the risk of using a cloud service. Other considerations must be addressed also, such as; How often the services will be unavailable? Can the user access their data when required? - The CSP currently do not willingly provide users will a clear answer for these questions. The loss of data or inability to access when required will have a knock on affect to the cloud user.

Cloud operators are able to transfer data across borders to different data centers if they wish. Again, such transactions and flow of data can lead to the data being vulnerable to malicious activities or being lost. The CSP should act appropriately and ensure that such circumstances do not occur. Given the ambiguous nature of cloud computing, currently that is no standardize regulation between countries over the ways in which a cloud service provider should be operating and storing user data. In an environment where protection is critical to a business the risk and threat of increased security breaches is reducing the trust between users and CSP, resulting in businesses considering alternative approaches to data storage than opting for a cloud. We are dealing with an immature technological structure - its benefits have been strongly marketed in recent years and security an afterthought. It is little wonder that businesses and governments have started to fear that cloud will not live up to the promises and expectations which the CSPs claim and create more issues they resolve.

4. Challenging Security issues

Attempting to define the correct level of security is difficult, as is forecasting the possible threats and how to prevent these in advance. According to Piper, [10] security is a balancing act, especially as no system is ever going to be 100% secure. It is a case of examining the need for investment and awareness to prevent serious security faults in the context of that particular environment. Risk assessment strategies to deal with problems must be highlighted and polices developed and understood to support the systems. Therefore the success, growth and reputation of cloud technologies is dependent on further research and assurance that security challenges are being examined and improvements are made to ensure a secure environment. Cloud providers play a critical role in addressing several challenges that affects security in the cloud. Due to the nature of a cloud environment there is an increase chance of vulnerability and attack than with other forms of IT systems.

A single point of failure can result in unauthorized access, data loss, performance failure and other security breaches. Security awareness and measures to prevent failures need to be continually improved as new technologies bring additional complications to existing systems. The fact that both Amazon and Microsoft have suffered serious problems with their clouds including services failure for a whole weekend in August 2011, when backup generators failed due to lightning strikes highlights the need for more protection. [11] This clearly shows the vulnerability of cloud systems. Given the fact that personal and sensitive data is being placed into the cloud, increased awareness of security and privacy is critical. The UK government is considering using a cloud system in the NHS [12] to store and transfer patients medical records. With the sensitive nature of information in medical records, it is essential that the government recognizes the dangers of using cloud rather than looking just at the possible economic cost benefits.

4.1Impact of deployment model

As mentioned earlier there are several different cloud service deployment models and ways in which they can be delivered to the end user. Therefore the type of security risk can vary. A user might not be aware of there different forms and their responsibility. For example, if a user discovers a security breach are they expected to resolve the problem or is the CSP? What will the impact be on the business? How can you find out what the ‘high’ security risks are for each form of cloud? Certain applications or business functions might not be suitable for deployment on a cloud. Therefore the business might have to consider keeping the existing system for some business functions and more the rest onto a cloud. This is going to impact the business finances as the business will be running two separate systems therefore cloud is not reducing costs.

4.2Cloud Deployment and Configuration

Configuration is a technique for logical integration of commercial or of the shelf components, in order to create systems with desired end-to-end functionality [19]. Configuration is the most critical process [20] of any heterogeneous network. It impacts the network in terms of security, performance, resilience, predictability. Misconfiguration is defined as wrong/incorrect configuration [21]. This can occur due to several different reasons - Delays in mapping configuration nodes, human errors, failure to follow or apply the correct policies, unaware changes to configuration parameters made, ITIL – hacking the dashboard, in capability of applications on a system, misconfiguration – from applications installation, and removal, misconfiguration due to security breaches. Not surprising, that several sources claim configuration errors are the biggest contributor to service failures. Between 40- 60% of downtime and other problems are due to configuration errors. Therefore, this evidence shows clod configuration is an area that requires regent attention.

4.3 Data security

In a traditional system, such as an extranet which was based within the business, data was resigned within the business boundaries which were maintained through that particular business security and access control policies. When it comes to using a cloud system for example SaaS, the data is stored outside the business boundaries and is placed in the hands of the CSP. Consequently the CSP should adopt additional security checks to ensure data security and prevention due to security breaches within applications, deployment and malicious attacks. However examples of security problems shows, this does not always occur. The end user is not with information regarding the security mechanisms and testing the CSP does. Therefore it is based on a level of trust between the user and CSP. Any vulnerabilities and accessed into the cloud could risk the data and have negative consequences on the business. Therefore cloud users cannot afford to just place 'trust' into their CSP without evidence of correct security processes and security mechanisms being enforced.

4.4Network security

As data is flowing between the business and the cloud provider it is essential that data flowing over the network is secured in order to prevent leakage of data or for a weak area be penetrated by an attacker. For example, if a security breach penetrates a cloud, it is harder to pin point the cause of the breach and locate it without hindering the security and performance of all users located on the cloud. Another consideration need to be that if data is vulnerable or lost how will the business know?

4.5Data availability and integrity

In order for businesses to operate effectively, it is critical that data is available when required. In a traditional system, the business may conduct regular backups of data as well as security testing, during periods such as evenings that will not hinder the daily operating of the business. However with outsourcing data into a cloud the CSP should conduct backups and upgrading. This might not be conducted as once as the user would expect This might have a negative impact on the business for example; increase the risk of data losses, reduce performance or prevent data being accessed when required. Data integrity is essential to a business. There has been several reports of security breaches that have compromised data integrity. Amazon S3 malfunctions led to users experiencing silent data corruption [13] over a period of time which compromised data. One of the main reasons why data integrity is compromises in cloud systems is because the data from the end user is transferred to the provider's storage systems which can result in the data being exposed to further malicious attacks during this remote transfer. The former CSP -LinkUp lost over 45% of data that they stored due to a system administrator error. [14] The business in question; creditability and reputation was seriously damaged, resulting in the business going burst. This has a significant impact on their users as many where unable to get their data back. It was not just a case that LinkUp was damaged but their cloud users suffered badly, resulting in financial ruin and loss of future customers.

4.6Data segregation and location

This leads to another important question potential cloud users must address - Where is your data being stored? This is becoming a concern for many cloud users since the high publicity of security breaches and data losses. Any business that is considering using a cloud system should conduct a risk assessment in order to assess if outsourcing data, especially confidential data will be protected by the CSP. The underlining objective of privacy regulations are to provide protection and ensure the privacy rights of individuals remain. However, maintaining an agreed level of protection is challenging. CSP needs to ensure they meet the different privacy restrictions on cross-border data transfer [15The lack of standardized regulations on privacy and protection has created major problems, especially in the adoption of cloud Therefore user's data might be protected in one country but not in another. Each country, or group of countries; such as those within the EU zone have their own form of privacy regulation. The difference between the legislations across the world is clearly noticeable through a comparison. The European Union (EU) privacy laws follow a strict and comprehensive approach which have been developed and influenced by the government and businesses within both the public and private sector. From this joint contribution, a framework has been developed which ensures the privacy codes of practice can be integrated within all sectors across the EU. EU favors very strict protection of privacy, while in US there tend to be a more relaxed approach to privacy legislation. US legislation tends to have no or limited government involvement. It is deemed the responsibility of businesses and industry bodies to develop specific industry sector legislations on privacy. This results in different laws being enforced on privacy across the US. Therefore the end user might be obeying laws in their home country but others do not have as strict regulations and privacy which can result in their data not being protected. By data being transferred across national boundaries and stored elsewhere, the user may in fact be at risk of privacy breaches without being. [16]Conversely, some users may be unwilling to store their data at sites in certain countries as local laws allow access to data for that country's government, such as the case with the Patriot Act in the US [1] [17]. This can also hinder the uptake of clouds

The lack of consistency within the US has led to the EU deeming the US as unsafe and lack's the necessary privacy protection standard expected. In an attempt to meet the concerns of the European, the US has recently developed the UK Safe Harbor Privacy Principles [18] which attempts to ensure US based businesses comply with the EU Directive 95/46/EC on the protection of personal data. By offering US businesses the option of registering to this in order to meet the European Union requirements has meant the EU still has concerns of the US privacy approaches and that this do not go far enough to protect EU users and their data. Other countries have little of less strict laws regarding data protection and security. Due to differences within economies and cultures it is difficult to vision a standard agreement global to protect users and businesses ever being developed

5. User Responsibility

Before deploying a cloud system, the business/user must select the most appropriate form of cloud based on their business and system use. Background investigation into different CSP their cloud services as well as internal and external factors and risks must be examined as part of the risk assessment.. It is essential that the business look at their existing systems and way up the pros and cons for using a cloud system based on what they have already. If the existing system is working well then why change to a cloud system? It is easy for businesses to get carried away and feel that they need to use the latest or most popular forms of technology to remain competitive. However as highlighted through examples of security breaches, cloud systems can be problematic and can result in major problems for businesses, especially if customer data is compromised. When examining different CSP businesses should request additional information and ensure that a service level agreement between the CSP to ensure their business requirements are understood and met.

Users need more information than simply reading the terms and conditions of their Service Level Agreement (SLA) contract. SLA do not provide sufficient assurances in regards to data privacy, data storage issues and third party involvement, as well as security breaches/ potential attacks and the effects. The business needs to establish the level of responsibility between the CSP and themselves especially if a security breach occurs –who is responsible? If the business does not feel that there is trust or is deeply concerned what the consequences to their business using a cloud system then make should consider alternative options to store data perhaps through an internal system which will mean they maintain control. A contract which includes the Terms of Service (TOS) and also s Privacy Policies and Service Level Agreement (SLA) will insure a level of assurance for users. This also provides grounds for legal action against the CSP if the provider does not maintain their side of the contract. For example, passing user details on to a 3rd party. It is also essential that users are aware of the data protection laws as their data could be transferred across into regions which are not as strict on data protection. This could result in invasion of privacy.

6. Moving the Cloud Forward

Besides the development and enforcement of privacy laws CSP should provide their own additional privacy and protection systems and mechanisms. Particularly as the CSP has a responsibility to the user to ensure they do their up must to provide a secure and reliable service. To prevent the loss of data, encryption techniques are critical to limit unauthorized access. All systems tend to have an identification and authorization system, which means the user have to login to their account to access data. This provides some form of security however further advancements in encryption techniques need to be present in cloud systems. A regulatory framework that enforces a set standard for CSP to comply needs to be developed. This will ensure CSP operate ethically and protect user rights to privacy. Further research and improvements within international privacy and protection laws **occurs,** resources and data sharing will continue to be risky. The failure of understanding the urgency for such measures, could result in a catastrophic economic impact as well have hindering the future developments and benefits of distributed systems across the world. Counter terrorism legislation needs to be produced as this will also influence the behavior of CSP and also give each countries power to take action against such crimes. Cloud privacy legislation should be customer – specific to ensure a level of guaranteed protection which would be outlined in the contract documentation between the CSP and user, regardless of the type of cloud service being provided. A regulatory framework that enforces a set standard for CSP to comply needs to be developed.

7. Future Work and Conclusions

This paper has explored some of the key security issues that remain in cloud systems. It is critical for the future development of cloud technology that concerns about security and privacy are addressed. This paper has highlighted the major concerns that are still features of cloud computing. Examples of security issues have illustrated these points, and backups up the argument that the increase in security threats and breaches has hindered users trust in CSP and therefore damaging the possible benefits that cloud can offer. It is difficult to see how cloud computing can be rebranded and CSP improve their image and regain trust with users. Until there are significant developments in legislation to protect users and data, as well as a standard security framework in the design and development clouds will continue to be heading the headlines over security breaches and data loss.

References

[1] Korri.T (2009) "Cloud computing: utility computing over the Internet" *Seminar on Internetworking 2009*

[2] National Institute of Standards and Technologies; Draft NIST Working Definition of Cloud Computing, May 14, 2009

[3] Mell, Peter; and Grance, Tim (2009). Effectively and securely using the cloud computing paradigm. Presentation to the 2009 Federal Information Systems Security Educators' Association Conference. March 26, 2009. Retrieved May 12, 2009, from csrc.nist.gov/organizations/fissea/2009-conference/presentations/fissea09-pmell-day3_cloud-computing.pdf.

[4] CIS 'Dutch government set to block US cloud IT providers' (20 September 2011) www.cio.co.uk

[5] Webwereld http://webwereld.nl/ [Accessed 20 September 2011]

[6] Cloud Business 'Lib Dems: Gov must look at security of public data cloud' (26 September 2011 www.theregister.co.uk

[7] Martyn Williams October 10, 2009 Microsoft loses Sidekick users' personal data http://www.computerworld.com/s/article/9139218/Microsoft_loses_Sidekick_users_personal_data

[8] Steve Musil (Feb 28 2011) Google blames software update for lost Gmail data http://news.cnet.com/8301-1023_3-20037554-93.html

[9] The Data Protection Act: Explained! http://www.dataprotectionact.org/

[10] Piper. F Keynote Speech "Information Security: It's a balancing act" The 5th International Conference for Internet Technology and Secured Transactions (ICITST-2010)
November 8-11, 2010, London, UK

[11] Matt Warman (08 Aug 20011) 'Amazon and Microsoft Cloud Services hit by lighting strike' www.telegraph.co.uk

[12] HotDesk (30 Jun 2011 'NHS launched cloud computing pilot' http://www.ihotdesk.com/article/800606888/NHS-launched-cloud-computing-pilot

[13] Amazon S3 Silent Data Corruption http://blogs.oracle.com/gbrunett/entry/amazon_s3_silent_data_corruption

[14] Rosenberg .D (2008)'All your cloud-stored data floated away at 'The Linkup' http://news.cnet.com/8301-13846_3-10015469-62.html#ixzz13HmBhMaU

[15] Pearson. S, (2009) Taking Account of Privacy when Designing Cloud Computing Services, in *Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing*, Vancouver, Canada, May 23 2009.

[16] Wood. K and Anderson. M (2011) 'Understanding the complexity surrounding multitenancy in cloud computing' ICEBE 2011 conference proceedings

[17] Mather, T., Kumaraswamy, S. and Latif, S. (2009) *Cloud Security and Privacy*. Sebastopol, CA: O'Reilly Media

[18] Safe Harbor Arrangement Official site http://export.gov/safeharbor/

[19]S. Narain, T. Cheng, B. Coan, V. Kaul, K. Parmeswaran, W. Stephens, Building Autonomic Systems Via Configuration, In Proceedings of Autonomic Computing Workshop, June, 2004

[20]Silveira. G, Silva.F (1998) 'A Configuration Distribution System for Heterogeneous Networks 1998 LISA XII, Boston, MA

[21]http://www.proz.com/kudoz/english/computers:_software/1057393-misconfiguration.html