Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

Internet cloud security: The illusion of inclusion

David Teneyuca

University of Texas at San Antonio, USA

ABSTRACT

Cloud computing has swelled into an estimated $46 billion market, representing roughly 17% of global software sales. This translates into a technology tsunami that can overwhelm the end user if they are not cautious about Internet safety. The ubiquity associated with cloud computing has created a huge false sense of security. Data, information, and applications are rapidly populating the "cloud environment". Society is experiencing the illusion of inclusion. They see the cloud as one service from one source. The general public has no notion of the perils that lurk in the cloud. The word haze may be a better description for this atmosphere. This article will describe and discuss cloud computing technology. Furthermore, it will examine what the cloud pioneers Apple, Google and Amazon, are doing to safeguard the cloud and how they cope with the illusion of inclusion.

1. Introduction

The rapid spread in cloud-based systems is heavily dependent on the development of Internet platforms. Online transactions such as e-marketing, m-commerce, and the general e-commerce models have provided useful opportunities to the business world. The Internet is the most important driver of cloud computing in the world today. The base principles of cloud-computing entail the data triad of confidentiality, integrity, and availability. However, with the advent of various web-based applications and portals, the posterity of cloud computing has been compromised. In essence, an "Illusion of Inclusion" is accepted by users of cloud technology. A level of comfort is present because of the paradigm that cloud security automatically includes the CIA triad. On the surface, the protection and safeguards appear sufficient, but it is only illusion. The Cloud Security Alliance (CSA) has identified several threats to cloud-based models and cyberspace in general (CSA, 2010). The massive implementation of cloud computing services should be done with certain reservations, in order to avoid falling victims of cloud security threats. Ubiquitous cloud computing and the aspect of global reach are key features of the Internet infrastructure. Unfortunately, these same features have attracted the perpetration of the mentioned cyber threats to the cloud-based systems (CSA, 2010).

2. Revealing the cloud

Apple and Google are positioning to cultivate their predictions and strategy on cloud-based media. The stakes are high. Digital delivery of electronic resources, for example their music and video industry, is on the increase for these key companies. The problem is that few in society comprehend what "the cloud" insinuates. All the same, these digital giants understand the victor will procure the biggest piece when portioning the profit pie. Forrester Research (2011) reports that $12 billion is expected to be spent in the U.S. market for personal cloud services. It is forecasted to serve 196 million end users. While most people are unknowingly using cloud computing, they are very apprehension over privacy, ethics, and security. A recent Ipsos (2011) report stated that nearly 40% of Americans feel that saving data to their hard drive is more secure and private than saving to cloud environment.

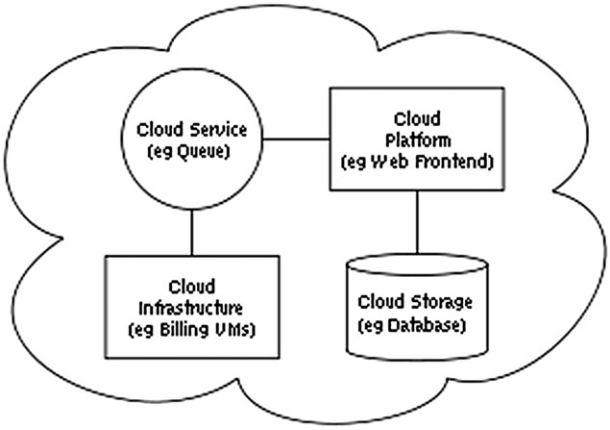
Cloud computing is a computer science terminology that means using the Internet and servers to secure and maintain

E-mail address: dteneyuca@msn.com.

1363-4127/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.istr.2011.08.005

data and its applications. The cloud computing technology allows business owners and consumers access to all sort of applications and their personal files over the Internet, without them installing any files at a computer with Internet access. This technology has increased computing efficiency by providing centralized storage of data. Cloud computing security is thus the application of all the sets of policies and controls in order to protect data and this should not be confused with the available security software that are cloud based. Without cloud computing the web server will run as a single computer or a group of owned computers, hence they will be powerful enough to serve a given amount of request per minute and with a certain amount of latency per request (Dhillon, 2007). But by joining this computer to a cloud, then the amount of requests will be far more than the web server can handle hence the response time of the requested pages will increase due to overloading.

With an organization adapting to cloud computing technology, it means that the organizational users will be using single-server power. This helps in conserving the computer power and different applications can be provided for the users and managed under the cloud server. This means that the user will not only download and install the application on their computers but all the processes will be stored and managed under the cloud server. The cloud computing model ensures "convenience and on demand network access to a shared pool of configurable resources" (Dhillon, 2007). Example: the networks, servers, storage device application and service which can rapidly process with minimal management effort. With cloud computing, all this work is done without the knowledge of the end user on the physical location of the system that is delivering him with the service. Consequently, the term cloud computing is associated with processing work from a known static place.



3. The cloud computing architecture

A more specific component of the computing architecture is known as the front end and the back end. Whereas the front end is the part that the clients or computer users can see and it includes the nodes and applications on the computer. These are what allow the user to gain access to the Internet via the end user interface from his personal computer. The back end comprises of different "servers, data storage devices and the computers" (Dhillon, 2007).

Companies like Yahoo, Microsoft, and Google have realized the benefits of this technology and proven that the technology is safe but with it risks. Cloud computing technology has played a great deal in the reduction of cost for both the system users and the website owners. This has made it possible for the user to access it from any point and still get the data they need while the site owner only needs to buy space in the server. More importantly, cloud computing allows automatic updates; the server gets the updates and applies it to anybody using the service without the user having to go to all the trouble of updating (Dhillon, 2007).

This technology has proven to be flexible and mobile. The user can work from anywhere in the world and only what is needed is a computer access and Internet connection. Cloud computing eradicates the issues of continuous downloading therefore saving time and the hard drive space since all a user needs is log in access to a network. Companies using this technology find it easy sharing resources thus saving businesses time and money. This is achieved by them placing their resources on a single network location that is easy for the worker to access. Benefits realized are securing of data and minimized loss of business files (Dhillon, 2007). With all the benefits been mentioned, there are security concerns that need to be addressed while relocating to cloud computing. These concern fall under the cloud computing providers and the client of cloud computing. Regrettably, this creates an illusion of confusion amongst the users.

The cloud computing providers must ensure that the infrastructure in use for the provision of cloud computing to the client and their data is secure and well protected. It's the duty of the customer to ensure that before transmitting sensitive and confidential information over the network, the provider has taken each and every security measure to guarantee the safety of their information.

4. Major security issues in the Internet and cloud computing platforms

In 2011 a survey on cloud computing was distributed. Cloud.com conducted a survey in the second quarter of 2011 to determine cloud computing usage trends among IT professionals who participated in the BitNami, Cloud.com, and Zenoss open source software and user communities. The results were collected from responses of 521 individuals as to their usage. It revealed preferences for virtualization and cloud computing technologies. The number one overall reason impeding cloud computing adoption was lack of cloud computing training (43%), followed by *security concerns* (36%). The Apple and Google are currently driving their strategies to include education about the cloud and easing consumer security concerns. They have to stay focused on overhauling user perceptions.

Confusing perceptions of the cloud require the companies to enhance the user's understanding of cloud's illusion of

inclusion, not confusion. For example, cloud supporters need to educate users or halt the misperception about the cloud platform. Apple chose to promote the cloud in its recent iCloud release, whereas Google downplayed the cloud in its debut. Apple's management decided to "brand it and own it for sure" according to Ipsos analyst Todd Board. Google adopted an approach where they "chose not to make cloud-specific references when it launched its cloud-based Chromobook tablet computers. They instead focused on verbiage as "nothing but the Web" to term their services.

Before implementing the appropriate security technique for the cloud, there are numerous security issues that must be considered. These risks include privileged user access, regulatory compliance, data location and segregation, investigative support and the prospects of a long-term viability (Graham, 2008).

4.1. *Privileged user access*

One of the most difficult elements to cloud monitoring in any database implementation is the activity of privileged users. In most cloud computing environments, there are unknown personnel at unknown sites with these access privileges. One way for Apple and Google to resolve this is through separation of duties, ensuring that the activities of privileged third parties are monitored by your own staff, and that the pieces of the solution on the cloud side of the network cannot be defeated without raising alerts. Apple and Google need the ability to closely monitor individual data assets (for example, a credit card table), regardless of the method used to access it.

The consumer data that is stored in the cloud platform faces the risk of unauthorized access by other cloud computing users. This is because the cloud environment may allow unauthorized users to bypass the physical and logical controls that are entitled for in-house handling (Graham, 2008). Apple and Google, intend to store sensitive data on the cloud. They attempt to gather enough information on the entities that are going to handle the cloud-based data. In addition, the cloud service vendors must be requested to state clearly all privileged data administrators who are allowed to handle the clients' information, hence the need for the establishment of a privileged user access technique. On the issue of privileged user access, the users should consider appointment of trustworthy administrators who can be allowed to handle the stored information.

4.2. *Regulatory compliance*

The cyberspace is governed by a number of standards and cyber laws. Thus, the cloud computing vendors are required to ensure complete compliance with the set audits and cloud certifications. For instance, the clients should strive to enquire whether the vendor is SAS 70 or ISO 27001 certified (Graham, 2008). In addition, the use of software licenses should be considered as a regulatory issue, since it involves the implementation of licensing regulations. The use of cloud computing user applications and the software must be done on the basis of mutual consent and permissions. Failure to follow the recommended software license procedures constitutes security risks (Graham, 2008).

Cloud computing not only affects SAS-70 and Sarbanes-Oxley (SOX) compliance. It can also impact Gramm-Leach-Bliley (GLBA), Payment Card Industry Data Security Standards (PCI DSS), and the Health Insurance Portability and Accountability Act (HIPAA). Compliance with regulations and standards necessitates differing levels of security. Due diligence is necessary to address compliance concerns by assessing SAS-70 reports. It promotes certification of the controls stipulated in the framework that would be in place if the data processing was not outsourced. Only one law is identified as specifically recognizing the role of a service provider—HITECH for HIPAA. All other laws and regulations leave all of the responsibility with the user For instance, encryption is necessary when transmitting HIPPA data over public networks. Since the concept of cloud computing is pushing data storage to the Internet, data needs to be stored in an encrypted format. Furthermore, compliance requires additional non-disclosure agreements and background screenings will be mandatory for any employees that have right to use to this information.

Google is identified in a recent report as not being able to state, definitively, where one's data is hosted or that its location will be restricted to any given region. Obviously, any opaqueness about location causes a real problem for users to ascertain if they are in compliance with applicable laws and regulations. Those who proclaim that cloud providers acknowledge responsibility for legal compliance measures fail to notice an obvious difficulty—cloud providers often do not know what data is being stored in their infrastructure. Thus they cannot know what legal conditions apply to the data.

4.3. *Data location*

The issue of data storage in the cloud should be assessed on the type of cloud. Data is located on private clouds. Alternatively, the location of sensitive and corporate data in the public clouds should be done on contractual commitments. People have been using the cloud concept to store data for a long time. There are millions and millions of photos in online galleries that use a cloud service. For example, Google's Picas uploads images on their photo-sharing site. In all honesty, the Google cloud is merely the countless locations to access Gmail and Docs. This is not the same as using Microsoft Outlook loaded on your personal computer and the Word application that saves the data to your hard drive. Google enhanced their cloud based office application. Chromebook is considered a dumb terminal. The laptop is need designed for saving documents on the local drive. Chromebook accessing data and stores it on the cloud environment. It should be noted that this also creates some concern because Google assumes that everyone has Wi-Fi at all times.

4.4. *Data segregation*

The cloud computing platform is a shared technology. Therefore, the storage of information and data should be adequately segregated to ensure that each client accesses only the necessary information, without affecting other customers' data (Graham, 2008). This security issue in the cloud platform requires the use of superior segregation methods, such as encryption and digital data signatures (Graham, 2008).

Moreover, the cloud vendors must provide adequate evidence to the customers that the encryption process was properly executed and tested by professional security analysts.

4.5. *Data recovery*

Data loss is a major security issue in the cloud platform. As such, the cloud computing service vendors must ensure that data recovery systems are put in place. The clients must understand the fate of their data, in case a disaster happens (Graham, 2008). Thus, one security requirement that must be fulfilled in cloud computing is the issue of data replication and the reliability of storage media. The restoration technology and forensic techniques must be embraced in order to ensure that data recovery aspect is appropriately addressed (Graham, 2008).

4.6. *Investigative support*

The cloud computing platform is complex in terms of legal investigations and enforcement of compliance aspects (Graham, 2008) (Graham, 2008). This security issue arises from the fact that data logging is done at separate locations and servers. The placement of computing responsibility on a single vendor is not possible, since the data may be co-located. The cloud platform comprises of several network hosts and data centers. However, the use of e-discovery applications can address the problem of investigative support. Customers should take part in the investigative process, in order to facilitate court proceedings in case of computing violations.

4.7. *Long-term viability*

When clients store their data and information in the private or public clouds, they should be convinced that the collapse of the service provider will not affect their data (Graham, 2008). Therefore, the issue of data transfer must be considered as a requirement in the storage of data in the cloud. Considerations such as the modeling of data files into importable applications should be made. The service providers must be vetted appropriately to determine their viability levels. This aspect promotes the aspect of data availability in cloud computing (Graham, 2008).

5. Security threats to cloud computing

5.1. *Threat to information privacy and confidentiality*

The Internet offers the aspect of global reach. On equal measures, this platform is characterized by lack of data privacy and confidentiality (CSA, 2010). Cloud computing is often invaded by malicious insiders, through service and account hacking. When unauthorized access to clients' accounts is made, erroneous manipulations can be perpetrated on data. With the frailties in security systems used by cloud service vendors such as Amazon and Microsoft Azure, several threats have cropped up (Jaatun, 2009). Data privacy and confidentiality on the Internet platform are done through Domain Name Server (DNS) spoofing, denial-of-service-attacks and also phishing (Jaatun, 2009). The use of insecure Application Programming Interfaces (APIs) enables unauthorized access to users' accounts to be a possible venture.

5.2. *Threat of shared technology*

The Internet is a shared infrastructure, a factor that has prompted the emergence of security threats in cloud computing (CSA, 2010). This sharing of the underlying cloud platforms enables the provision of online products in a scalable way, but the security issues associated with this practice are robust. This threat is often perpetrated on the disk partitions, CPU caches and the compartmentalization components (CSA, 2010). The multi tenancy offered by the Internet has attracted malicious activities on these underlying components by hackers, thereby paralyzing the online operations of other users (CSA, 2010). For instance, the Red and Blue Pill root kit developed by Joanna in 2006 proved to be capable of destroying the Internet and cloud computing platforms such as CPU caches and GPUs (CSA, 2010).

5.3. *Threat to data loss and leakage*

The exposure of clients' data to other cloud computing users can lead to data loss and leakage (Jaatun, 2009). This threat is perpetrated through improper encoding and encryption of data files or encryption. The cloud service providers may fail to seek the consent of data clients when deleting or altering electronic records. In addition, the lack of secure software keys and frail authentication processes can also lead to loss or leakage of sensitive corporate data in the cyberspace (Jaatun, 2009). According to the CSA, the current data retention strategies that are used over the Internet platform are not efficient (CSA, 2010). Unauthorized access to user accounts has become a common practice due to the use of weak access control and API infrastructures. Data transmission has suffered the threat of network access through spoofing. In this process, hackers often monitor the user network access and spoof the MAC addresses.

Companies like Google, Amazon, and Microsoft are the forerunners in using cloud computing technology. Just like any form of technology it has had its fair share of challenges: ranging from government intervention in foreign countries and attacks from hackers and they have been able to rise up from these challenges by securing and encrypting their servers through the SLL technologies and upgrading of their firewalls. With the support of stable operating systems like UNIX, Google has been able to secure its E-mail system. With the flexibility and fixing of the security loopholes, cloud computing technology has proven to be a great success.

6. Mitigating cloud computing security threats

6.1. *Data encryption*

There are various ways through which the Apple and Google security threats can be mitigated. However, data encryption is the best practice of enhancing privacy and confidentiality as

essentials of cloud computing (Jaatun, 2009). In addition, this process can be enhanced by subsequent generation of digital signatures which allow for a consensual handling of data in transit. Encryption entails providing a specific key for data access. In the recent past, the use of Advanced Encryption Standard (AES) has helped in ensuring safety of data in transit (Jaatun, 2009). In this standard, symmetric and asymmetric data authentications are used. Unlike the public key cryptography, the asymmetric encryption involves generating two distinct keys which are meant for use by the data sender and the recipient (Jaatun, 2009).

The well-liked Rivest Shamir Adelman (RSA) encryption can also play an important role in digital signature generation. In this process, data can be decrypted appropriately from cipher text through the use of signature verification (Jordan and Bruno, 2011). Majorly implemented by Microsoft Azure and Apple, the RSA encryption has reportedly improved network interfaces and data transmission in the electronic payment cards. Through the generation of symmetric encryption keys, the RSA standard has particularly enabled the transmission of various multimedia contents over the Internet (Acquisti et al., 2010). This is because it ensures an uninterrupted exchange of private keys which are used in the access of data. The Voice over IP (VoIP) technology has specifically benefitted from the provision of digital signatures over the Internet platform (Acquisti et al., 2010). The encryption keys ensure that data transmitted from the VoIP source to the specified destination is adequately secured.

6.2. *Preventing network intrusion*

Network intrusion is the cause of various malicious activities over the cloud platform (Jordan and Bruno, 2011). However, there are various technologies which can be used in preventing this kind of intrusion. The Multiprotocol Label Switching (MPLS), Virtual Private Networks (VPNs) and Virtual Local-Area Networks (VLANs) are some of the best strategies that have been developed to avoid this problem (Jordan and Bruno, 2011). These technologies enable a reliable path isolation to take place. In the MPLS-VPN process, isolation is performed through routing network devices to a Virtual Routing and Forwarding (VRF) system (Jordan and Bruno, 2011). This process ensures that the devices can only access a virtually secured network that is free of possible intrusions.

6.3. *Spam filtering, phishing detection and blacklists*

Security threats to mobile e-commerce are on the increase. As a result, the mobile agents in cloud computing have developed additional security enhancement services, such as filtering and blacklisting of suspicious contents (Oberheide, n.d). Spam filtering is mostly used for securing text contents, such as SMS and email messages. The filtering process enables in detecting the source of malicious information, through extracting the IP addresses of the senders (Oberheide, n.d). In some countries like China, the use of content filtering and blocking has enabled the security of web contents. This is done through deleting any content deemed inappropriate by the cyberspace authorities (Oberheide, n.d).

Phishing detection, widely deployed by Google, has helped in curbing the phishing attacks which lead to hacking of users' accounts (Oberheide, n.d). Google uses this security service through a number of anti-phishing tools which can detect the presence of a counterfeit websites. In the mobile e-commerce platform, these anti-phishing solutions have helped in enhancing the security of e-commerce transactions through the provision of secure Internet platforms (Oberheide, n.d). Fraudulent activities have decreased in Google's Apps Engine, since the phishing detection process has significantly been enhanced. Several phishing attacks that were reported in the year 2009 in Google are now a thing of the past (Oberheide, n.d). This is because the detection processes have been enhanced in order to improve the online business transactions.

Another additional security service that can help in mitigating Internet attacks is the creation of a centralized blacklist (Oberheide, n.d). Despite the low levels of implementation in this system, global centralized blacklists can help in blocking or eventual grounding of websites which are created to extort online shoppers (Oberheide, n.d). Cloud computing can benefit from this venture through device-level implementation, which can greatly reduce the chances of malicious operations over the Internet. Over the past years, there are various websites that have been labeled insecure for cloud computing.

7. Cloud computing and principles of security

There are fundamental principles of security that cloud computing needs, in order to make guarantees to its users. These are: confidentiality, integrity, availability, authenticity, and information security and users privacy. Cloud computing technology users need to be assured of confidentiality when using the system. Confidentiality involves assuring the customer that there information will not be disclosed with or without their authority. This is important even to the companies that use cloud computing and transact their business online and it could involve the use of credit cards. This security principle needs to be considered since business and organizations will lose their customers if not assured of the security of their personal information (Dhillon, 2007).

The cloud computing technology has achieved in dealing with data integrity. Companies like Amazon and Google who use this form of technology have managed to withstand Internet attacks from hackers who try to gain access to information being transmitted over the network. Availability in relation to computer science and technology is a process of ensuring that information is readily available to the end users wherever they need it. In order for this to happen, cloud computing makes use of the security controls in protecting data while extending the communication channels. This has helped in preventing the denial-of-service attacks (DOS).

With the growing of technology, many companies are shifting to online businesses. Thus it is important to authenticate the data transactions, communications and documents moving across the networks to ensure that they are genuine and free from malicious computer virus. Cloud computing has tried in guarantying this factor. The next security principle is the non-

repudiation. This happens when two or more parties are involved in a transaction over the Internet and one party happens to claim or deny receiving the transaction. The use of digital signatures through authenticity and non-repudiation can be used to challenge this form of claims. With the usage of cloud computing services to store information, the customers are in full exposure to potential violation of their privacy.

There have been cases where, Yahoo and Google mail users have been exposed to these attacks and their personal privacy violated. The possession of user's confidential information is only entrusted to the cloud service providers, and any hacker access to this information could affect the relation between the cloud computing service providers and its users (Dhillon, 2007). In cases or situations involving the use of wireless cloud computing, the customer safety risk is high and considered to increase. With exposure of personal information and of recent a new security threat has been realized through international or cyber espionage. Another great security threat is during data migration within the cloud service provider. This takes place when the user wants to switch or change the cloud providers. A set standard between operators does not exist and the change process is known to be complex and this can result given the scenario when the cloud service provider is declared bankrupt thus may lead to exposing the users.

8. Conclusion

The robust implementation of cloud computing models has benefitted many organizations and individuals in a myriad of ways. However, the security threats and risks that exist in the Internet platform have compromised data privacy, availability and confidentiality. Some of the cloud computing threats include data loss, leakage, shared technology threats, service and account hacking operations among others. There are various ways of mitigating these problems in the cloud platform. Users need to stay away from the cloud confusion. Data encryption and the generation of digital signatures can help in ensuring security for data in transit. These processes entail the provision of a secret access key to both the sender and the recipient on the data files. Other methods of ensuring security include the use of VPNs, MPLS, and spam filtering solutions.

Apple, Amazon, and Google have provided many security features for the cloud environment. Unfortunately, people remain unswerving. In their eyes there is no concern over lost information or privacy of the data. Conversely, industry experts point out the risk is mitigated by having copies or backups available to the user. Saving data on personal devices is exposed to theft, loss, or physical damage to the device.

REFERENCES

Acquisti A, Smith S.W, & Sadeghi A. Trust and Trustworthy Computing: Third International Conference, TRUST 2010 Berlin, Germany, June 21–23, 2010 Proceedings. New York: Springer Heidelberg; 2010.

Cloud Security Alliance (CSA). Top threats to cloud computing V 1.0. Retrieved June 3, 2011 from: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf; 2010.

Dhillon G. Principles of information systems security text and cases. New York: John Wiley & Sons Publishers; 2007.

Graham DT. Negotiating contracts that will keep our cloud afloat. you're going to put that in a cloud?. Retrieved June 5, 2011 from: http://itm.iit.edu/netsecure11/DanielGraham_CloudPresentation.pdf; 2008.

Jaatun M.G. Cloud computing: First international conference, CloudCom 2009, Beijing, China, December 1–4, 2009 Proceedings. New York: Springer Heidelberg; 2009.

Jordan S, Bruno A. CCDA 640-864 official cert guide. Indianapolis: Cisco Press; 2011.

Oberheide J. (n.d). Virtualized in-cloud security services for mobile devices. Retrieved June 3, 2011 from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.169.5857&rep=rep1&type=pdf.