Journal of International Technology and Information Management

Volume 22 | Issue 4 Article 3

11-4-2013

Is Security Realistic in Cloud Computing?

S. Srinivasan
Texas Southern University

Is Security Realistic In Cloud Computing?

S. Srinivasan
Jesse H. Jones School of Business
Texas Southern University
USA

ABSTRACT

Cloud computing is rapidly emerging as an attractive IT option for businesses. As a concept cloud computing is well received because of the benefits it offers but many users are not clear about the scope of security in cloud computing. Many surveys point out that security in the cloud remains the top concern for many businesses in their decision making consideration in spite of the cost advantages it offers. In order to identify the security concerns we analyzed over 50 research articles and industry white papers published over the past five years. In this paper we focus on the question "Is security realistic in cloud computing?" In presenting the justification that it is possible to expect adequate security features in the cloud we address several related issues. In this context we first briefly describe the three types of cloud services – SaaS, PaaS and IaaS. Then we focus on the security aspects that businesses must pay attention to in order to succeed. Next, we consider the importance of trust in the service providers and how they could build customer trust in their services. This discussion leads to service reliability in the cloud and what the cloud providers have learned from cloud outages in order to build trust. Also, we highlight how the security features offered in the cloud support compliance requirements. We conclude the paper with some relevant information on the legal aspects related to cloud computing.

INTRODUCTION

Cloud computing today is benefiting from the technological advancements in communication, storage and computing. The basic idea in cloud computing is to take advantage of economies of scale if IT services could be provided on demand with a decentralized infrastructure. This idea is a natural evolution from the IT time-share model of the 1960s and 1970s. Today, technology has advanced significantly and many more organizations have computing demands that are elastic in nature. Organizations large and small require reliable computing resources in order to succeed in business. Large businesses deal with complex systems where as Small and Medium sized Enterprises (SMEs) need access to affordable computing resources. Based on these aspects we can summarize some of the rationale for today's cloud computing needs as follows:

- acquiring and managing the IT resources requires specialized skills,
- maintaining a reliable IT infrastructure is expensive,
- rapid technology advancements make it difficult to keep current the IT expertise,
- internet has opened up many opportunities for individuals as well as small businesses,
- number of entities requiring computing resources has grown exponentially,
- SMEs' demand for computing resources varies significantly over time,
- providing data security is a complex undertaking.

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

In the above paragraph we have identified some of the major reasons as to why cloud computing would be advantageous to use. When a significant part of the business depends on a type of service that the business does not fully control, the question arises as to how the business can meet its obligations to its customers. As highlighted above, IT services are essential to the success of the business but it would be cost prohibitive for the business to manage an IT center with the required expertise and fluctuating demand on resources for processing and storage. Thus, a business using cloud computing must understand the security challenges that it would be responsible for and how cloud computing could help in this regard. We address the security challenges by first noting the differences in the types of cloud computing that a business might be using.

In order to address the security challenges associated with cloud computing, we need to understand first the meaning of cloud computing. The primary reason for this is that the term 'cloud computing' is used as a catch-all for a wide ranging array of services. After a careful analysis of numerous sources in the literature we have arrived at the following working definition of 'cloud computing' based primarily on the National Institute of Standards and Technology definition: *Cloud computing consists of both the infrastructure and services that facilitate reliable on-demand access to resources that can be allocated and released quickly by the user without provider intervention using the pay-as-you-go model* (NIST, 2011). It is worth noting in this context that Mell and Grance further amplified on this general definition in their NIST report that is now widely accepted as one of the important definitions of cloud computing (Mell, 2011).

Today's cloud computing has three basic types: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In the simplest of terms 'cloud computing' has come to embody SaaS. Similar to the IT time-share model mentioned earlier, SaaS provides both the server hardware and software to an organization without any of the complications of managing an IT system. The simplest example of SaaS service would be email for an organization. The cloud provider benefits from the economies of scale in managing a large infrastructure because of their strength in that area and is able to provide the necessary computing resources to the user, majority of who are SMEs, at an affordable cost. SaaS leaves the full control of the computing system with the provider. Some of the major commercial SaaS providers are Amazon, Google, Microsoft and SalesForce.

PaaS provides the customer a platform, such as the Windows operating system with the necessary server capacity to run the applications for the customer. PaaS is used mainly by developers who need to test their applications under a variety of conditions. The PaaS cloud service provider manages the system for its upkeep and provisioning of tools such as .NET and Java whereas the customer is responsible for the selection of applications that run on the platform of their choice using the available tools. Thus, the customer is responsible for the security challenges associated with the applications that they run. For example, a customer running a SQL Server database on the platform should be aware of the vulnerabilities of the database system. Hence, the customer should have the expertise to manage such applications on the platform used under this pay-as-you-go model. The benefit to the customer is that if their hardware needs change or if they require a Linux/UNIX platform for some other applications,

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

then provisioning them takes only a few days as opposed to few weeks to make the new system operational. Major PaaS cloud service providers are Google App Engine and Windows Azure.

IaaS provides the customer the same features as PaaS but the customer is fully responsible for the control of the leased infrastructure. IaaS may be viewed as the computing system of the customer that is not owned by them. Unlike PaaS, IaaS requires the organization to have the necessary people with extensive computing expertise. The IaaS customer would be responsible for all security aspects of the system that they use except physical security, which would be handled by the cloud provider. Amazon and IBM are examples of IaaS providers. Combining the information presented so far about these three types of cloud services with additional cloud service providers, we have Table 1 that provides a quick snapshot of the available resources.

Table 1: Summary of cloud service providers.

Provider	Type of service	Product name
Amazon	SaaS	AWS
	PaaS	Elastic Beanstalk
	IaaS	EC2, S3
Google	SaaS	Gmail, GoogleDocs
	PaaS	App Engine
Microsoft	PaaS	Azure
Salesforce.com	SaaS	Sales Cloud
	PaaS	Force.com
Rackspace	PaaS	Rackspace Cloud
	IaaS	Rackspace Cloud
IBM	SaaS	CloudBurst
	IaaS	Blue Cloud
EMC	IaaS	Atmos
Apple	SaaS	iCloud
AT & T	SaaS	Synaptic Hosting
VMware	IaaS	vCloud Director

It is worth noting that these three types of services are gaining ground. According to the Ponemon Institute/CA Technologies 2011 study, among cloud service providers, SaaS accounts for 55 percent, PaaS accounts for 11 percent and IaaS accounts for 34 percent. Besides these three service types available, a potential user must also consider the four different cloud deployment models for meeting their computing needs. The four cloud deployment models are public cloud, private cloud, hybrid cloud, and community cloud. The most common cloud deployment model is the public cloud. In the public cloud the customer shares the resources with other customers. On the other hand, in a private cloud the resource are dedicated to the organization and has greater security because the computing resources are not shared with other customers. Private cloud is affordable only for large organizations. A natural evolution from public cloud and private cloud service models is the hybrid cloud which uses both proprietary computing resources and/or private cloud resources that the organization manages directly and the public cloud for some of the computing requirements, especially the ones with varying

demands on resources (Bhattacharjee, 2009). Two of the major hybrid cloud providers currently are VMware and HP. Another important statistic to note is that 65 percent of the cloud service customers use public cloud service while 18 percent each use private cloud and hybrid cloud services. These three types of cloud services aim to meet the customer requirements at different levels of engagement in managing the computing hardware and software. This has a direct correlation to the size of the organization in choosing the type of cloud service. For this reason we can broadly classify the cloud computing users as belonging to either the public cloud or the private cloud. Small and medium sized businesses typically use the public cloud and large organizations use the private cloud. All the cloud service providers mentioned earlier provide both public and private cloud services. In the private cloud, a large organization which has a data center to manage, is able to use large amounts of storage and computing power dedicated to just their organization only. The private cloud facilitates the large organization to handle demand elasticity similar to the public cloud provider.

The community cloud is used by organizations with a common focus such as health care, automotive and financial services. The community cloud represents a vertical market in which the organizations stand to benefit by having a dedicated server that addresses the specialized needs of that sector. For example, in the media industry companies are looking for ways to simplify content production at low-cost. This requires collaboration among a large group of people. A community cloud facilitates the location of necessary computing resources for content production and editing. By using a community cloud dedicated to the media industry this need is met. Windows Azure platform is used as a public cloud for this community cloud architecture.

Having provided a brief overview of the three basic cloud types and the four deployment models, let us next review the security aspects in the cloud as discussed in several research articles and industry white papers. One of the main reasons for the cloud to provide cost efficiencies is its ability to leverage the economies of scale in their hardware and their ability to offer Virtual Machines (VMs) on a single hardware for multiple clients. Moreover, cloud providers enable visibility to the customer on the location of their VM in the cloud. How this feature is exploited by attackers to launch side-channel attacks on the cloud is the major contribution of Ristenpart, Tromer, Schacham and Savage (2009). In their oft cited paper "Hey, You, Get off of my cloud," these UC San Diego and MIT researchers highlight the security concerns of many businesses. They point out the data leakage aspect in a public cloud (Ristenpart, 2009). In a multi-tenant environment on a physical infrastructure, which is very common in a public cloud, such attacks are capable of extracting encryption keys. Thus, one of the heavily relied upon defense to secure data storage in the cloud becomes vulnerable. Armbrust et al., discuss in their paper the top 10 obstacles to cloud adoption. These UC Berkeley researchers show the current status of the cloud service and how the technology needs to improve further to address customer security concerns. This paper points out how, in spite of advancements in interoperability among different platforms, the storage APIs tend to be proprietary. This basically locks in a cloud customer from switching to another cloud service provider easily (Armbrust, 2010). Providing very high reliability of service in the cloud requires extensive infrastructure deployment with plenty of redundancy built-in. Major service providers like Amazon, Google, Microsoft and Salesforce have the ability to assure very high availability of their services. All these services have experienced some well publicized outages which cause concern for businesses in their desire to switch to the cloud.

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

The significance of cloud security is the focus of one of the four parts of the book Cloud Computing by Antonopoulos and Gillam. In this edited book the authors have included several chapters on cloud security (Antonopoulos, 2010). In particular, the work of Durbano, Rustvold, Saylor and Studarus focus on the significance of standards in enabling cloud security. Their work points out the gaps in ISO 27002 security controls (Durbano, 2010). Chen, Paxson and Katz answer the question of 'What is new about cloud computing security?' Their analysis shows that many of the cloud security issues are not really new except that they hinge upon multi-tenancy trust considerations and auditability of service providers' ability to back up their claims with data on security aspects (Chen, 2010).

One of the challenges for any new technology is the availability of global standards. Cloud computing is evolving rapidly but there are not many commonly accepted standards yet. ISO 27001, NIST and Cloud Security Alliance are all working toward providing guidelines for the cloud industry. One of the Cloud Security Alliance guidelines involves the Top 9 Cloud Computing Threats in 2013. Some of these threats relate to data breaches in the cloud, data loss due to data leakage, insecure APIs and abuse of cloud services (Cloud Security Alliance, 2013). We already pointed out one such abuse from the work of Ristenpart et al involving side channel attacks. Next we look at the literature review article of Yang and Tate in which they classify 205 articles that appeared in cloud computing (Yang, 2012). They started this line of research in 2009 when they reviewed 54 articles. Since then the field has grown significantly and they included several of the articles that we are examining in this brief review. Similar to Yang and Tate's work, Idziorek and Tannian surveyed all research articles in the area of public cloud computing and focused on cloud computing security. This article points out several reasons on the impediments still facing cloud computing adoption (Idziorek, 2012). Likewise, Modi et al surveyed the issues affecting cloud computing adoption and their vulnerabilities. This paper identifies some solutions to strengthen security and privacy in the cloud (Modi, 2013). Related to this work is the technical book by Trivedi and Pasley on Cloud Computing Security. As developers of cloud security solutions with a major technology company these authors identify several security solutions based on cloud architecture, design and the way the customers deploy their cloud based solutions (Trivedi, 2012). Continuing this line of research on cloud computing security, Zissis and Lekkas propose the creation of a trusted third party focused on cloud security. The authors point out that this arrangement would create a security mesh for all cloud users that will lead to a trusted environment (Zissis, 2012).

Many businesses use cloud computing for data storage. This feature provides the business a cost effective solution to store as much data as necessary and at the same time provide related data backup, recovery and business continuity benefits. However, it also introduces the risk of not having full control over the data storage as it is physically outside the control of the business. This has led to several risks for businesses. To address this concern Wang et al propose a flexible distributed method. In their approach they propose a method that achieves storage correctness and supports dynamic operations such as data update and delete (Wang, 2009). John Viega from a major security service firm analyzed the security aspects of the three major cloud services – SaaS, PaaS and IaaS. His analysis shows that in the case of SaaS the main concern for the customer relates to the service providers' ability to protect the infrastructure from attack and ensure non-leakage of data in the multi-tenant environment. In PaaS, even though the developers who subscribe to this service will be able to develop their own security solutions, they are still

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

dependent on the service providers' way of protecting the service below their application level for intrusion prevention. For IaaS, the major concern is the way the virtual machines are configured. A related concern with IaaS service is the reliability of the service provider (Viega, 2009). Mark Ryan has a special focus in his paper on privacy concerns related to the cloud because his paper addresses an area of interest for many academic researchers. The goal of Ryan's paper is on the privacy aspects related to the two major conference management systems in use – EDAS and EasyChair. The paper highlights the many benefits of the conference management systems on the cloud and also highlights some concerns such as the leakage of reviewer information, cumulative success records of many researchers related to their submissions for a variety of conferences over a long period of time and aggregated reviewing profile of the reviewers. These data could be accidentally or maliciously disclosed by systems administrators on these cloud systems where they are privy to large volumes of data. Even though this is a very small segment of the cloud service industry, this paper's focus is on the potential privacy concerns for data stored on the cloud (Ryan, 2011).

The next set of papers that we examine relates to cloud computing risks and how they are addressed. Gartner Research identifies seven cloud computing risks that are quite common. These are presented in the context of a potential cloud customer evaluating a cloud service. Some of these concerns relate to how the service provider handles privileged access to system resources, their regulatory compliance activities related to physical security of the system and third party audit such as SAS 70 Type II audit report, where they store the data and how they segregate belonging to different customers so that they do not co-mingle (Brodkin, 2008). In summarizing the cloud security concerns of many European partners, Daniele Catteddu in his lengthy report points out that the two major benefits of cloud services, namely the economies of scale and the operational flexibility are 'both a friend and foe.' The main thrust of this report is that the cloud customer needs an assurance that the service providers are following sound security practices to mitigate the risks faced by the customer and the provider (Catteddu, 2010). Similar to the above report, the World Privacy Forum developed a report on the privacy implications of data stored in the cloud. This report especially focuses on the many legal aspects of compliance based on laws such as HIPAA (Health Insurance Portability and Accountability Act), GLBA (Gramm-Leach-Bliley Act), ECPA (Electronic Communications Privacy Act), and Fair Credit Reporting Act. The report notes that the information stored by an individual or a business with a cloud service provider may have less protection than when the same information is held by the information creator. Moreover, governments find it easy to obtain lot of information from a centralized source such as a cloud provider (Gellman, 2009). The main contribution of this report is in raising the awareness of the cloud customers relative to privacy issues in the cloud.

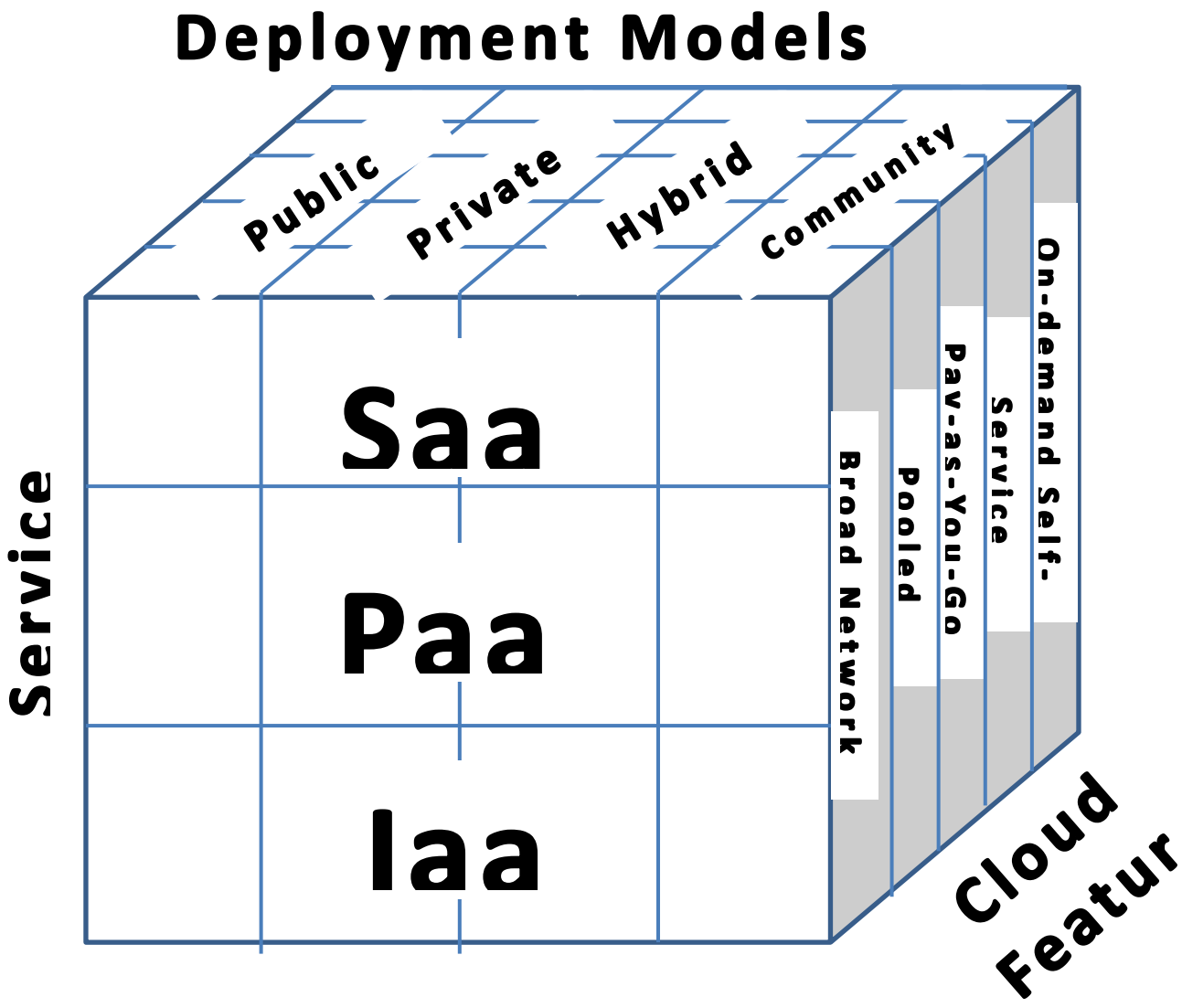
One of the indicators of a mature model is the availability of enough case law to understand how courts interpret the technological aspects. Using this metric cloud computing is not yet mature enough to have a solid body of case law. To understand the ambiguities of how to interpret the implementation models in the cloud we cite two instances. In the first case, Cartoon Network sued CSC Holdings (parent company of Cablevision) for copyright infringement in 2009. In this case, Cablevision provided customers the ability to store the recordings of their choice on the cloud and access the same using their authentication credentials. Cartoon Network contended that Cablevision was violating their copyright by sharing their content with others using the

cloud storage. The court ruled that Cablevision was simply providing their authenticated customers a storage facility in the cloud and not illegally sharing any copyrighted material. In the second case, Arista Records sued Usenet.com in 2009 for violating their copyright on their musical content by enabling unauthorized redistribution of their copyrighted content through the bulletin board system in the cloud managed by Usenet. The model used by Usenet enabled the cloud users to share their stored content with others unlike the Cablevision case. Since the cloud was used in this case for data sharing the court ruled that it was a copyright violation by Usenet (Wittow, 2011).

The analysis so far was focused on the US experience with the use of cloud computing. However, cloud computing is a global phenomenon. In United Kingdom the government's cloud computing initiative is known as G-cloud. In the brief article focused on G-cloud and NIST definitions of cloud computing, author Craig-Wood develops a comprehensive picture of all aspects of cloud (Craig-Wood, 2010). We have developed Figure 2 based on this view. This figure summarizes effectively our prior discussion on the three cloud types, four cloud deployment models and some of the major advantages of cloud services. Just as cloud computing is used in UK, the Australian experience relative to the legal requirements of the cloud provider is described in their white paper by Vincent and Crooks. The details presented in this white paper relate to privacy laws, location of data in the cloud, how foreign governments might get access to this data, security beaches and service availability (Vincent, 2013). These are all important security considerations for a cloud service consumer to consider prior to making a commitment to use the cloud.

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

Figure 2: Cloud Types-Deployment Models-Features.



We review next the German experience with respect to cloud computing based on adherence to privacy laws. This topic is discussed by Doelitzscher, Reich and Sulistio in their Cloud Security Project with particular emphasis on Small and Medium-sized Enterprises (SMEs). They introduce a six layer security model that involves risk analysis and encryption (Doelitzscher, 2010). We conclude this security review of existing cloud computing literature with a brief outline of Bhensook and Senivongse's assessment of security requirements compliance by service providers. This paper makes an extensive analysis of Cloud Security Alliance's recommendations by using the Goal Question Metric (GQM) for security requirements compliance. The weighted scoring model that they develop is then tested using Amazon Web Services' (AWS) compliance. The results show that in most cases AWS is compliant with various metrics being measured (Bhensook, 2012).

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

NEW PARADIGM

Cloud computing is a significant shift in the way IT services are managed. Organizations large and small have managed IT services over the years with varying levels of investments. Today, with advancements in communication technology, many new options have opened up for existing businesses and new entrepreneurs want to use more of the capabilities of IT. These two aspects have spawned the significant growth of cloud computing, which gives the customer the ability to benefit from the pay-as-you-go model. Cloud computing has enabled the service providers to benefit from the economies of scale.

This change in service rendering is necessitated by the fact that today's workforce is increasingly mobile and consequently the need for access to remote resources is greater. Moreover, demand fluctuations for IT services are a reality. Businesses cannot afford to provision IT services to meet peak demand, which occur infrequently. Cloud computing provides an ideal solution to meet these needs without incurring significant cost in services provisioning.

Investments necessary to have a reliable IT service kept many prospective entrepreneurs from creating online ventures. On the web, businesses large and small look alike. Cloud computing is providing entrepreneurs the opportunity to try their ideas out, with IT services no longer holding them back as a barrier to entry. The major beneficiaries of cloud computing are small and medium sized businesses as this new concept provides them an opportunity to try out high-end services with no up-front cost, allowing them to use the pay-as-you-go model.

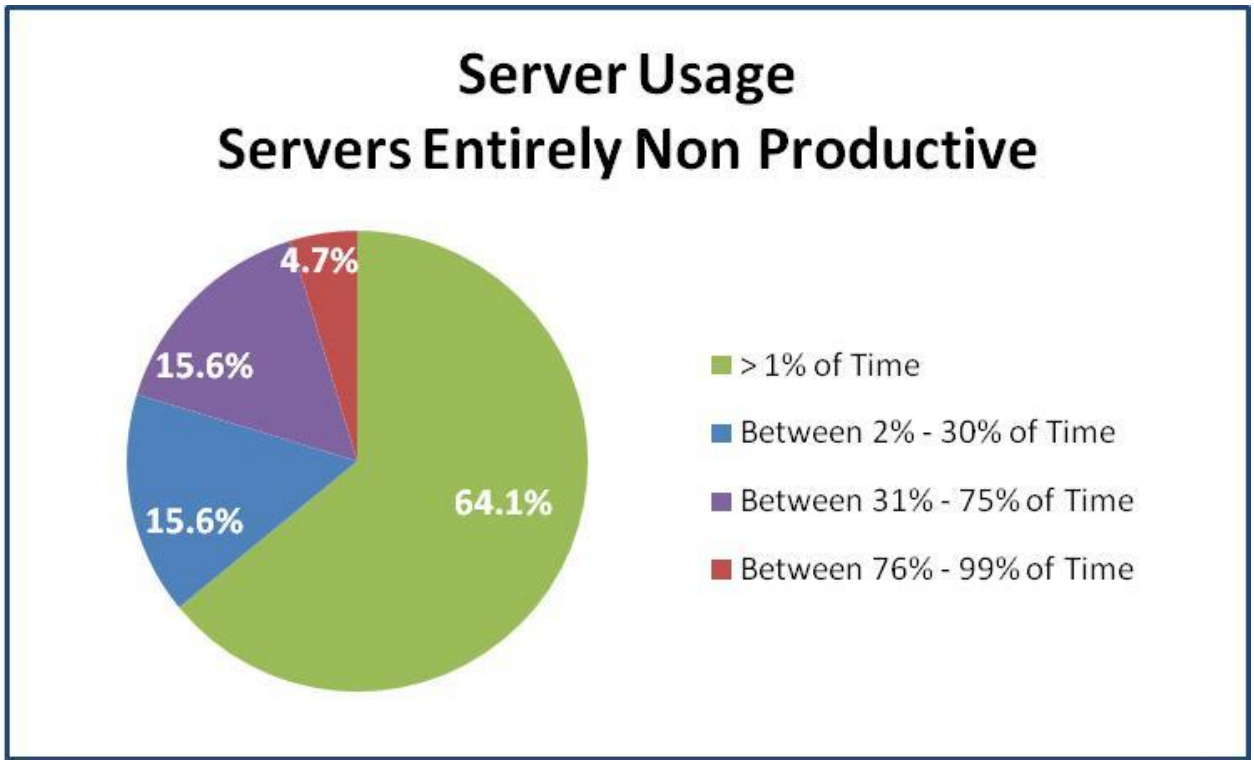
Large enterprises also stand to benefit from cloud computing, although of a different nature. Large enterprises manage data centers and the IT paradigm shift referred to earlier mean more in the context of accessing data from the data centers. In this context private clouds have been introduced where the benefits of storage management and elasticity in demand for computing services are the key drivers. Moreover, the cloud technology also offers high level of reliability and availability of systems without significant capital layout. Often, the benefits of cloud computing are realized by taking a hybrid approach. The hybrid approach gives the large organizations the ability to manage their IT centers and at the same time expand their computing capacity without large capital investment by utilizing the cloud resources. This is especially useful to meet seasonal peak demands with hybrid clouds. Organizations with seasonal high demands that could benefit from hybrid clouds are in the entertainment industry around holidays, sports networks with on-demand service and tax service providers.

In assessing cloud computing's appeal we should consider the usage levels of organizational servers. Server utilization level gives a good metric to see if the investment cost in hardware is worth it. The U.S. federal government started looking at the server utilization in its data centers several years ago and found that the utilization level was low. According to a 2010 report by the Computer Sciences Corporation (CSC), a global technology services company, that among all data centers in use the server utilization rate is between 6 percent and 20 percent. The data from this report is shown in Figure 2.1. Even Google's server utilization rate is around 40 percent. One reason for the low utilization is the lack of virtualization and the need to use dedicated servers for multiple operating systems as well as separation of sensitive applications. Cloud

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

computing is a natural fit to address the low utilization aspect because of high levels of virtualization. With multiple users sharing the computing resources, cloud computing has a very high level of server utilization (Hayes, 2008).

Figure 2.1: Server Usage Statistics.



Cloud computing architecture enables businesses to meet demand elasticity in computing resources. Business organizations have great difficulty in dealing with demand elasticity for cost considerations. A useful model to compare here is how networks manage elasticity in bandwidth demand. For cost reasons network bandwidth provisioning uses the Committed Information Rate (CIR) model. Likewise, cloud computing provides a similar feature in meeting demand elasticity in both storage and computing power. Without the ability to meet demand elasticity, businesses may end up with an underprovisioned service. In that case customers would abandon such services. Jeff Bezos, CEO of Amazon, highlights the success of extreme demand for computing power within a very short period of time. In this case a nascent web services company, Animoto, grew so rapidly that its server needs grew from 50 to 3,500 servers over a three day period. Amazon was able to accommodate such a high demand easily. This is a good illustration of high demand elasticity.

In the traditional model, the end user had control over the creation, maintenance and deletion of a document. In the cloud environment, the end user is spared the trouble of maintaining the computing system and reaps the benefits of the application software. This is a positive aspect of cloud storage. However, it is not entirely clear to the end user that when a document is deleted it is going to be inaccessible from the storage system. There have been instances where the

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

document lingered on in the storage system of the cloud provider. These types of issues are unique to cloud computing and thus are a departure from the standard expectation of a computer system. Thus, we note that a shift in approach is needed in order to have control over the online information.

Many large organizations are considering cloud based services as a cost-effective way to plan for disaster recovery. In this case the organization has its own computing resources that it controls and plans to use the cloud services for disaster recovery purposes. In the traditional model for disaster recovery the organization would use a warm or cold site as its backup facility, which is a recurring expenditure for the company. The cloud model eliminates this recurring expenditure, instead the organization pays for the services it uses when needed. The main cloud service type being considered for disaster recovery is IaaS. Data backup is another service area for which cloud computing is gaining ground. In the traditional model companies perform an incremental backup daily and full backup weekly. The backed up data gets stored off site and handled by companies such as Iron Mountain. In the cloud computing model a large organization would use the cloud services for backup and recovery, which by its very design is at an offsite far away from the company location. The organization could architect the backup process in such a way that it is an automated full backup continuously. The promise of these two services in the cloud has brought Microsoft and Iron Mountain together to offer data backup and recovery. Using the Windows Azure platform Microsoft performs data backup and Iron Mountain manages the stored data for the customer based on their expertise in this field. The customer pays for this service based on the amount of storage used and the retention period for backup data. This service has the added benefit of offsite storage built-in that is essential for disaster recovery and backup because the cloud provider is remotely located relative to the customer. An essential component of efficient data backup is data de-duplication, also known as 'intelligent compression.' The de-duplication method allows for storing only one copy of the data and providing a pointer from all future occurrences of the same data. Data de-duplication can be performed at the file or block level. The latter is more efficient than the former. In typical email backups many users may have the same file as an attachment and so the same file is backed up multiple times. Using the de-duplication approach only one copy is saved and all other references point to the same copy. This is a typical file level de-duplication. Most often de-duplication is more efficient at the block level. In this approach each block of data is hashed using MD5 or SHA-1 and the index is stored. Future hashes of blocks producing the same index are treated as duplicates and not stored. There are sophisticated methods available to detect hash collision, which is rare (Armbrust, 2010).

SECURITY CHALLENGES

Managing security is a major challenge to both large and small organizations. Transitioning to cloud computing increases the challenges faced by these companies many-folds because of the several unknowns. One important aspect of security is physical security. An organization that owns the computing resources knows how to provide physical security. An organization that uses cloud computing does not know where the physical resources are located and so providing that form of security is transferred to the service provider. This raises the important question of liability in the event of a security compromise. Many organizations do not take this aspect into consideration in their security planning. Ultimately it would be the organization that would be

held accountable by its customers for any security loss due to failure in physical security. Major providers such as Amazon, Google, SalesForce and Microsoft provide the necessary physical security guarantee.

Security and trust are closely related. An important contributor to trust is transparency. One way to achieve customer trust in cloud environments is to share the security practices as they relate to physical security, backup and recovery, compliance, incident handling and logs of security attacks. With the help of non-disclosure agreements cloud providers can share details of logs on incident handling and security attacks. Information security's core requirements are confidentiality, integrity and availability. We add the fourth piece – access control – to this security scenario. In this section we will explore the various security challenges facing a customer using cloud computing.

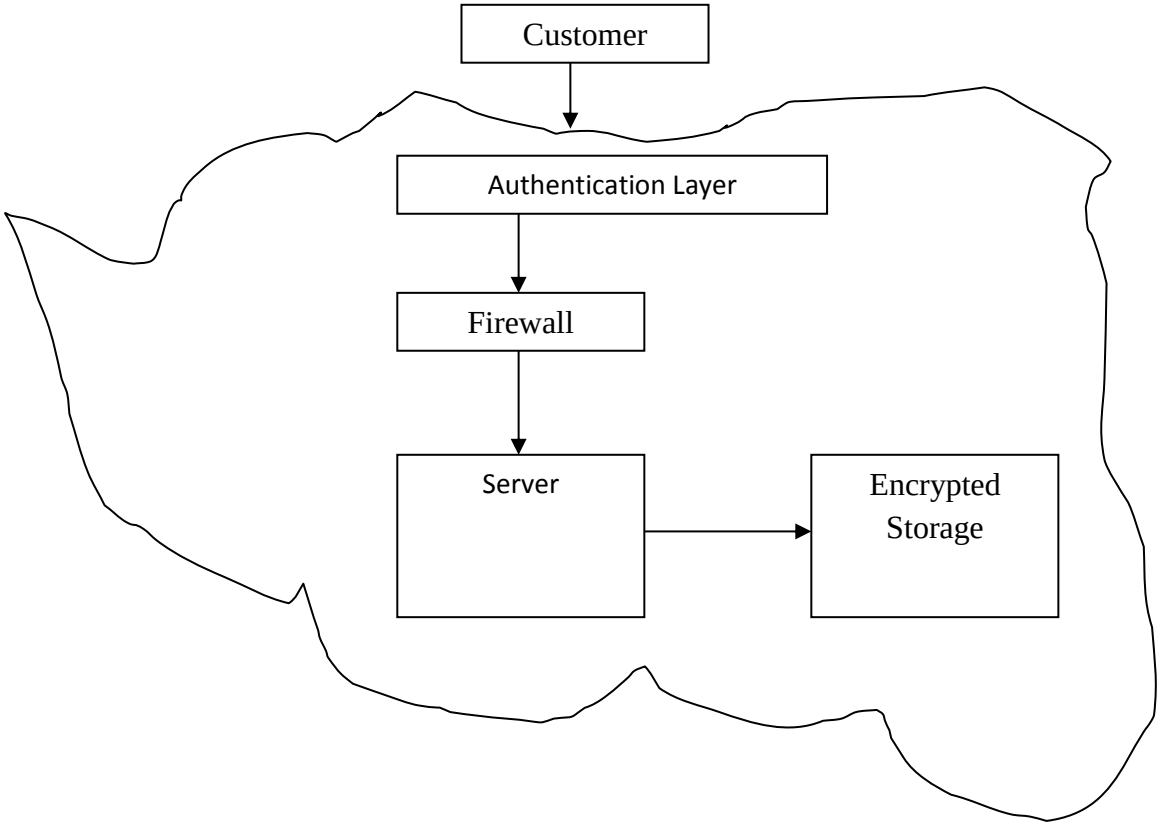
First and foremost, the cloud customer must understand the levels of security the provider is guaranteeing. This includes system up time, system upkeep with respect to software updates and patches and sharing a variety of logs that will enable the cloud customer to meet certain compliance requirements such as HIPAA and SOX. Since the cloud provider manages the servers on which the customer applications run, access control to the applications is an important part of security as well. Access control in cloud environments differ based on the type of service – SaaS, PaaS, IaaS.

Today's cloud environment is dominated by SaaS and in this case the cloud provider should provide the necessary authentication mechanisms to grant access. The leading SaaS service is CRM, estimated to be about US$ 3.8 Billion worldwide in 2011. A Goldman-Sachs survey in 2010 points out that small and medium sized businesses would consider cloud service 70 percent of the time and would prefer a cloud solution, if available, 58 percent of the time. This high level of confidence in SaaS cloud services shows the maturity of this particular market.

The success of cloud computing as a viable alternative to individual businesses managing their own IT centers is commendable. From an operational perspective this is an efficient model. However, from a security perspective there are several major concerns to overcome. As mentioned above, physical security of systems is one concern. A more serious concern is in access control – physical access to hardware, privileged access to operating environment, access to application software. In Figure 3.1 we combine the access control feature with the type of protection that a service provider could guarantee the customer for security of their data in this design. The goal of this proposed architecture for cloud relative to the cloud customer is to provide a way for them to see how their data and interaction with the cloud are both secure. The Authentication layer inside the cloud provides a way for the cloud customer to control who gets access to their virtual machine and data. Knowing who the privileged users are from the service provider perspective will enable the customer to monitor the access log, which they should be able to get in an automated manner from the service provider. The firewall inside the cloud gives the cloud customer the level of assurance that they are accustomed to in their own systems. The customer would be able to have the firewall configured by the service provider the way they want, thus giving an added level of protection to their data. By using encrypted storage in the cloud and holding the encryption key themselves, the customer will have added security protection in case of data leakage because of storage comingling.

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

Figure 3.1: Cloud Computing Security Infrastructure.



From a security perspective cloud computing should be viewed as a potential single point of failure. Cloud providers have high redundancy in their architecture, yet relying solely on one cloud provider may raise reliability issues. Moreover, when many customers are still ranking cloud security as their main concern in their switch to cloud computing, the providers have to offer many trust building measures. One such is system reliability. This has suffered some setback because of some well publicized instances of cloud outage. Some of these major outages are the April 2011 Amazon AWS failure (Amazon, 2011), October 2009 DDoS attack on Bitbucket that utilized Amazon EC2 and the November 2007 Rackspace failure due to power supply disruption. Since reliability could still be an issue for some customers, one possible solution to using cloud services is to split the types of cloud services among multiple service providers. A common approach to this could be to use one cloud provider for operations and another provider for storage solutions.

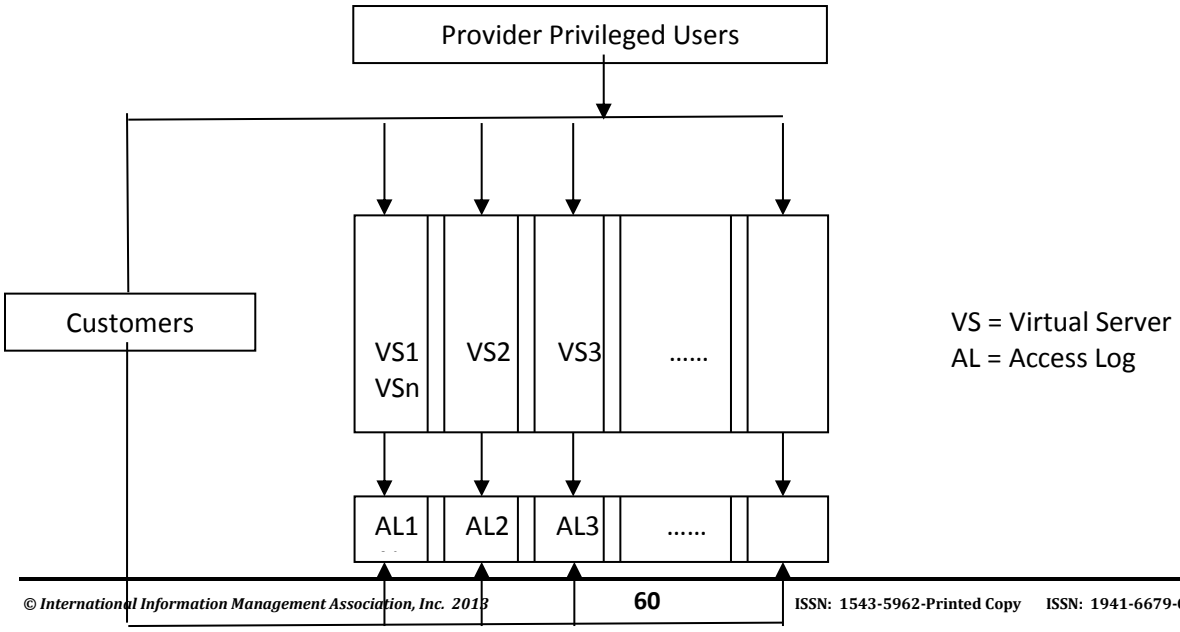
Besides the access control concerns with cloud storage and the violations cited in this regard, it is a major decision for a customer to have a data backup outside of the cloud service provider. The reason for this is that when a cloud service provider has to comply with law enforcement demand for removal of a storage device for investigative purposes, many other customers might also be affected. This is not a hypothetical scenario. In March 2009 a data center in Dallas owned by a cloud service provider was raided by law enforcement and as such many other customers were also affected because their data was unavailable for access for an extended period of time.

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

Security, interoperability and portability are considered the major barriers for cloud computing adoption. In many instances the cloud service provider does not think it is their responsibility to protect customer data. In the 2011 Ponemon Institute/CA Technologies cloud security study a surprising finding is reported (Ponemon, 2011). It points out that a majority of the cloud service providers do not think that cloud security is their responsibility and even more disturbing is that these providers do not think that their services protect and secure customers' sensitive data. Cloud service customers should be aware of how secure their sensitive data are and how to protect the same.

Cloud computing model requires virtualization in a big way. In virtual environments data comingling is a reality. We identified in Figure 3.1 how a customer could work with the service provider in establishing a level of security to prevent comingling of data on a central server. Since cloud service providers operate in a multi-tenant environment in their public cloud, an unintended consequence of comingling data from multiple customers on the same physical device is data leakage. The author recommends the architecture specified in Figure 3.2 as a preferred solution to cloud provider's infrastructure vis-à-vis the customer need for access logs. The figure shows the need for virtualization of servers and isolation of the virtual servers. Also, the customer should be aware of the privileged users at the cloud provider who will have access to their virtual servers as well as the ability to get data from user access logs for their respective virtual servers in an automated manner. Ristenpart et al have highlighted the data leakage problems associated with comingling data on the same physical device (Ristenpart, 2009). Data leakage could lead to privacy violations. When cloud providers do not see that it is their responsibility to protect customer data, as highlighted by the Ponemon Institute study, it puts an extra burden on cloud customers to use encryption for all their data. We expect more and more customers are going to be sensitive to the potential of data leakage from the cloud, which is not a problem if they had their own computing resources. The security does not come from encrypted storage alone. The customer must hold the encryption key in their system at their place of business and not place it on the cloud, even if it is in their virtual server. Ristenpart et al have shown how an attacker could place their virtual server on the same physical server as the customer and perform side-channel attacks to recover the encryption key.

Figure 3.2: Cloud Provider Infrastructure.



In order to provide data security, both customers and cloud service providers must realize that security has to become information-centric, i.e., security moves with the data. This way any operational decision by the cloud service provider will protect the customer data. Another important aspect of handling the cloud security challenge is to trust the processes and infrastructure. To this end,

1. Businesses should know from cloud provider how the following are handled:
   - Physical security
   - Number of privileged users with access to hardware
   - Log data for system access, up time, incident handling, attacks on the system
   - Data backup and recovery
   - Compliance with regulations
2. Security and trust are interrelated
3. Important contributor to trust is transparency

The significance of compliance such as SAS 70 Type II Audit builds trust for the customer.

Providing data security involves not only having adequate measures but also compliance with relevant laws. In order to verify compliance an organization would require log data related to access control and incident handling. The cloud customer should be able to get such data from the provider. This is not standard practice with the cloud providers. System up time is another issue that should be looked into by the cloud customer. The system up time could be verified only with log data. In Table 3.1 we highlight the compliance aspects from Amazon and Google, two of the major cloud service providers.

Table 3.1. Summary of Security Features by Amazon and Google

Provider	Security Features	Compliance Support
Amazon	• ISO 27001 certified • SAS 70 Type II Audit certified • PCI DSS Level 1 certified • FISMA certified • Physically secure data centers distributed around the world • User control for data encryption • Data backup • Customer-aware storage region • Does not allow third-party cloud providers • Processes in place to prevent unauthorized insider access to customer data • SLA guarantee of 99.95% up time • Supports multifactor authentication	SOX compliant GLBA compliant HIPAA compliant

	• Supports host-based firewall	
Google	SAS 70 Type II Audit certified Multi-layered physical security Hardware customization, maintenance Secure storage handling Privacy protection for customer data Data centers located around the world Redundancy built into storage management Ease of movement for customer data into and out of Google Apps Provides additional levels of access control designed by customers	Google does not explicitly certify any of their products as meeting standard compliance requirements such as HIPAA, SOX, GLBA, FISMA, etc. Instead, it provides features that customers can enable in order to be compliant on their own using Google Apps.

Trust aspects include knowing the reliability of cloud service. To this end the cloud service provider should be able to provide the customer their infrastructure capability with respect to system uptime. It is an integral part of knowing the provider's ability to assure security. Table 3.2 gives the amount of downtime allowed when cloud providers claim a certain level of uptime, usually denoted by a set of 9s. For example, four 9s means 99.99 percent up time. Highly available computing is expensive. Addition of one 9 to the guaranteed uptime nearly doubles the cost. Given these limitations the cloud provider uptime claims should be backed by data.

Table 3.2 : System downtime chart based on up time claim by cloud provider.

System Availability	Maximum downtime Per year
99.999%	00:05:15
99.99%	00:52:35
99.9%	08:45:56
99%	87:39:29

Source: Stratus.com

Standards play an important role in security. In the case of Cloud Computing, the standards are still evolving. The groups that are making contributions to cloud standards are the Distributed Management Task Force, Object Management Group, National Institute of Standards and Technology, European Telecommunications Standards Institute and the Storage Networking Industry Association. These standards help address the issues raised earlier so that customers can be familiar with the level of security that they are getting from the cloud provider.

FUTURE OF CLOUD COMPUTING

Cloud computing has many benefits to offer. Foremost among them is in meeting the elasticity of demand and the ability to use the 'pay-as-you-go' model. Cloud computing is often referred to as "converting capital expenses to operating expenses." Cloud computing provides risk transference for the customer in that the customer need not worry about the cost involved in overprovisioning or under provisioning resources. It is important to note that a business that consistently under provisions resources will lose customers permanently.

Cloud computing has become the preferred storage solution to deal with Big Data. We are seeing an exponential growth in data due to several social media applications. A welcome contribution to cloud computing has been added by Google through its MapReduce architecture. MapReduce provides a simple way to process large volumes of data quickly. The open source implementation of MapReduce method is Hadoop by Apache. Many organizations use Hadoop Distributed File System (HDFS) to process large volumes of data in a reliable way. Without the availability of cloud services many businesses will not be able to afford the high cost of infrastructure needed to use Hadoop. Handling security in the cloud is a complex process and many researchers are working on incremental aspects of providing security to a variety of aspects in cloud processing. Hamlen et al (Hamlen, 2010) discuss one such security solution for the cloud. In particular, they discuss ways to efficiently store data in remote locations and query encrypted data. This approach to storing data in the cloud after encrypting it provides a level of security for sensitive data. Some of the cost advantages that the cloud provides will be lost if we were to add the cost of encryption. If we store data in the cloud in encrypted form then we need to develop processes to query encrypted data. Hamlen et al use HDFS for virtualization and apply Hadoop processes for secure storage.

Another area where cloud computing could play a major role in the future is in backup storage. Many businesses do not consider backup as highly critical and with cloud services providing a viable low cost alternative, it is expected to catch on in the future. Companies like Carbonite and CrashPlan have simplified the process of backup. Recovery goes hand-in-hand with backup and customers are responsible for the policies regarding recovery testing periodically. Given the cloud infrastructure capability this should be a simple solution as the customer would be able to have access to the necessary hardware and software available to test the recovery aspects on a pay-as-you-go model.

As cloud computing emerges as an affordable service for many businesses it is inevitable that there will be several legal issues that arise as to ownership of data, liability for protection of data and safeguarding of privacy. There is not a large body of case law in this regard. We cite two recent court cases where challenges were mounted because of the use of cloud service. In the first case, Cartoon Network challenged that CableVision's Remote Storage DVR service violated the Copyright laws. The CableVision service offered the ability for the customer to record shows and store them in the cloud in their personal storage area for later playback. Since the access to this storage was based on customer's access control mechanism of userID/Password, the court ruled that CableVision was not violating the Copyright laws (Cartoon Network, 2008). According to a study by Harvard University's Lerner and others, the impact of this ruling was significant as it resulted in investments of over a billion dollars in this area of cloud service. However, there were conflicting rulings in Europe (unfavorable in France, favorable in Germany) on similar aspects of storage in the cloud by individual users (Borek, 2012).

Cloud service technology has the ability to allow each user of their service to have their own storage space as described in the CableVision case above. The cloud technology is also capable of storing a single copy of an artifact and make it available only to authorized users. MP3Tunes, a new cloud-based music service, created a locker in which a customer could place a song and access it later on demand with appropriate authentication. As part of the cloud technology's

capability, MP3Tunes held only one copy of a music in the locker even when new users attempt to store the same song. Capitol Records, one of the largest music companies, sued MP3Tunes as offering a music distribution without proper license of copyrighted material. The Manhattan District Court in U.S. ruled that MP3Tunes did not violate the owner's copyright for the song (Capital Records, 2011) as it was leveraging one aspect of the technology known as deduplication. The users accessing the song all had stored that song in the cloud. These two cases point to the challenges faced by the cloud service industry as the service matures.

SUMMARY

Cloud computing is efficient and cost effective. It takes the burden out of many businesses to maintain a technical system and yet reap the benefits of its availability. In our analysis so far we were able to identify the many security challenges posed by the cloud service. The solutions identified in various places in the above discussion show that we can answer in the affirmative the question raised by the title of this paper concerning cloud security. Cloud computing has opened up the opportunity to many entrepreneurs to focus on their core business and count on cloud services to provide the necessary computing power. Many businesses experience demand elasticity and cloud computing is a natural fit in providing cost effective service in this area. Security aspects did not get much attention for a few years now and many customers were focusing on availability of service. As more and more businesses start using this service the question of security is coming to the forefront. We have addressed some of the security concerns with cloud computing. One area that is bound to receive greater attention is in compliance with government laws in each jurisdiction in which the cloud operates and the global industry requirements such as the one by the Payment Card Industry as many businesses depend on cloud computing.

REFERENCES

Amazon. (2011). AWS Security Center. http://aws.amazon.com/security/ Accessed 11/15/13

Antonopoulos, N., & Gillam, L. (2010). Cloud Computing: Principles, Systems and Applications. *Springer: London, UK.*

Armbrust, M., Fox, A., Grith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. & Zaharia, M. (2010). A view of cloud computing. *Communications of ACM*, 53(4), 50-58.

Bhattacharjee, R. 2009. An Analysis of the Cloud Computing Platforms, *MIT MS Thesis*, Cambridge, MA.

Bhensook, N., & Senivongse, T. (2012). An Assessment of Security Requirements Compliance of Cloud Providers, *Proceedings of the IEEE 4th International Conference on Cloud Computing Technology and Science*, 520-525.

Borek, C., Christensen, L., Hess, P., Lerner, J. & Rafert, G. (2012). Lost in the Clouds: The Impact of Copyright Scope on Investment in Cloud Computing Ventures, http://www.intertic.org/Conference/Lerner.pdf Accessed 11/22/13

Brodkin, J. (2008). Gartner: Seven Cloud Computing Risks, http://www.idi.ntnu.no/emner/tdt60/papers/Cloud_Computing_Security_Risk.pdf Accessed 11/15/13.

Capital Records vs MP3Tunes. (2011). Manhattan U.S. District Court, 1:07-cv-09931.

Cartoon Network vs CSC Holdings. (2008). US 2nd Circuit Court Ruling, 536 F .3d 121.

Catteddu, D. (2010). Cloud Computing: Benefits, Risks and Recommendations for Information Security, *Web Applications Security*, edited by Serrao, C., Diaz, V. A. & Cerullo, F., Springer: Berlin, Germany.

Chen, Y., Paxson, V., & Katz, R. H. (2010). What is new about cloud computing security. *UC Berkeley Technical Report* EECS-2010-5.

Cloud Security Alliance. (2013). http://www.cloudsecurityalliance.org Accessed 11/15/13

Craig-Wood, K. (2010). Definition of Cloud Computing incorporating NIST and G-Cloud views, http://www.katescomment.com/definition-of-cloud-computing-nist-g-cloud/

Doelitzscher, F., Reich, C., & Sulistio, A. (2010). *Proceedings of the 10th IEEE International Conference on Computer and Information Technology*, 930-935.

Durbano, J. P., Rustvold, D., Saylor, G., & Studarus, J. (2010). Securing the cloud, *Cloud Computing*, edited by Antonoupolos, N. & Gillam, L., 289-302, Springer: London, UK.

Gellman, R. (2009). Privacy in the clouds: risks to privacy and confidentiality from cloud computing. *World Privacy Forum*.

Hamlen, K., Kantarcioglu, M., Khan, L., & Bhavani, T. (2010). Security Issues for Cloud Computing, *International Journal of Information Security and Privacy*, 4(2), 39-51.

Hayes, B. (2008). Cloud Computing, *Communications of ACM, 51*(7), 9–11.

Idziorek, J., & Tannian, M. (2012). Security analysis of public cloud computing. *International Journal of Communication Networks and Distributed Systems*, 9(1&2), 4-20.

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing, *NIST*, Gaithersburg, MD.

Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey on security issues and solutions at different layers of cloud computing. *Journal of Supercomputing*, 63(2), 563-592.

NIST SP 800-145. (2011). The NIST Definition of cloud computing. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf Accessed 11/15/13

Ponemon. (2011). Security of cloud computing providers study, *Ponemon Institute*, May.

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, *Proceedings of 16th ACM Conference on Computer and Communications Security*, Chicago, IL.

Ryan, M. D. (2011). Cloud Computing Privacy Concerns on our Doorstep, *Communications of ACM*, 54(1), 36-38.

Trivedi, K., & Pasley, K. 2012. Cloud Computing Security, *Cisco Press*: Indianapolis, IN

Viega, J. (2009). Cloud computing and the common man. *IEEE Computer*, 42(8), 106-108.

Vincent, M., & Crooks, K. (2013). Cloud Computing: What legal commitments can you expect from your provider? *White Paper*, SheltonIP, Sydney, Australia, 1-21. http://i.haymarket.net.au/Assets/cloudcover2013.pdf Accessed 11/15/13

Wang, C., Wang, Q., Ren, K., & Lou, W. (2009, July)). Ensuring data storage security in cloud computing, *17th International. Workshop on Quality of Service*, 1-9.

Wittow, M. H. (2011). Cloud Computing: Recent Cases and Anticipating New Types of Claims, *The Computer and Internet Lawyer*, 28(1), 1-8.

Yang, H., & Tate, M. (2012). A descriptive literature review and classification of cloud computing research, *Communications of AIS*, 31(2), 35-60.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3), 583-592.

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy