ISSN:0975-9646

Cloud Computing Environment-Legal Obstacles

Sumeet V. Vinchurkar[#1],Ajay A. Jaiswal [*2]

[#]*Assistant professor, Department Of Computer Technology, KDK College Of Engineering, Nagpur*
[*]*Associate Professor, Department Of Computer Technology, KDK College Of Engineering, Nagpur*

Abstract: As today's world deals with the moving and handling of the big data, and securing such data through legal implication is important. Cloud means providing services on large volumes that can migrate through national borders. As the legal issues are the uncertain as it varies different for different localities, business and technologies. This paper deals with the legal issues to provide privacy to data in cloud environment and suggest the integrated solution certainty and clarity to the legal uncertainties pertaining to data.

Keywords: personal data, cloud, cloud computing, security, legal.

1. INTRODUCTION

In early 2000s, organization started spending money to set up their IT infrastructure for improvement of business application, by purchasing own dedicated server. As the days progresses these sever became virtual and easily available publically through internet, and here the 'cloud' born [1]. Cloud Computing [2] is distributed environment as to provide on demand computing resources and services operated by centralizes server resources on a scalable platform. End user can use cloud services in terms of application, infrastructure or platform provided by Cloud service providers (CSP's). Cloud computing is a model can easily be manageable accountable and configurable. In general cloud providers offer three types of services i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

To understand the concept of cloud computing in the most basic sense, let's look at a physical world example [1]: Imagine four employees of a company availing car pooling services. The car in which they travel from their respective homes to their office can either belong to any one of them or they may avail services of a third party car pooling company. In case of the latter, the ownership of the property (car) does not belong to the employees, however, they own the articles (such as bags, laptops, documents, etc) which they carry along with them in the pooled car. They pay the car pooling company for availing the transport services as per their actual usage and the car is available to them as and when required by them. Similarly, the essential characteristics of 'cloud computing' are;

- *Pay as per use;*
- *Use it 'as and when required';*
- *Services provided by a third party service provider;*
- *No change in the ownership of the main property.*

Further, in a cloud computing environment, a cloud can either be a 'public cloud' or a 'private cloud', similar to one of the employee owning the car (or joint ownership of the car by all four employees) or the car pooling service owning the car respectively. While essentially the end result of using a public cloud or a private cloud remains the same, there is a slight difference between the two. A public cloud offers cloud computing solutions to almost anyone who has access to the internet and generally at no or low cost. On the other hand, a private cloud is typically a private data center/network that offers cloud computing solutions to a limited number of identified users at a certain or shared cost.

There are also four different cloud deployment models [2] namely Private cloud, Public cloud, Hybrid cloud and Community cloud. Details about the models are given below.

Private cloud: Private cloud can be owned or leased and managed by the organization or a third party and exist at on-premises or off-premises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user's access and the networks used are restricted. One of the best examples of a private cloud is Eucalyptus Systems.

Public Cloud: A cloud infrastructure is provided to many customers and is managed by a third party and exists beyond the company firewall. Multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically provision resources. These clouds are fully hosted and managed by the cloud provider and fully responsibilities of installation, management, provisioning, and maintenance. Customers are only charged for the resources they use, so under-utilization is eliminated. Since consumers have little control over the infrastructure, processes requiring powerful security and regulatory compliance are not always a good fit for public clouds. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used. Public cloud providers such as Google or Amazon offer an access control to their clients. Examples of a public cloud includes Microsoft Azure, Google App Engine.

Hybrid Cloud: A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other. These clouds would typically be created by the enterprise and management responsibilities would be split between the enterprise and the cloud provider. In this model, a company can outline the goals and needs of services . A well-constructed hybrid cloud can be useful for providing secure services such as receiving customer payments, as well as those that are secondary to the business, such as employee payroll processing. The major drawback to the hybrid cloud is the difficulty in effectively creating and governing such a solution. Services from different sources must be obtained and provisioned as if they originated from a single location, and interactions between private and public components can make the implementation even more complicated. These can be private, community or public clouds which are linked by a proprietary or standard technology that provides portability of data and applications among the composing clouds. An example of a Hybrid Cloud includes Amazon Web Services (AWS).

Community Cloud: Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider and rarely offered cloud model. These clouds are normally based on an agreement between related business organizations such as banking or educational organizations. A cloud environment operating according to this model may exist locally or remotely. An example of a Community Cloud includes Facebook which is showing in figure 1.

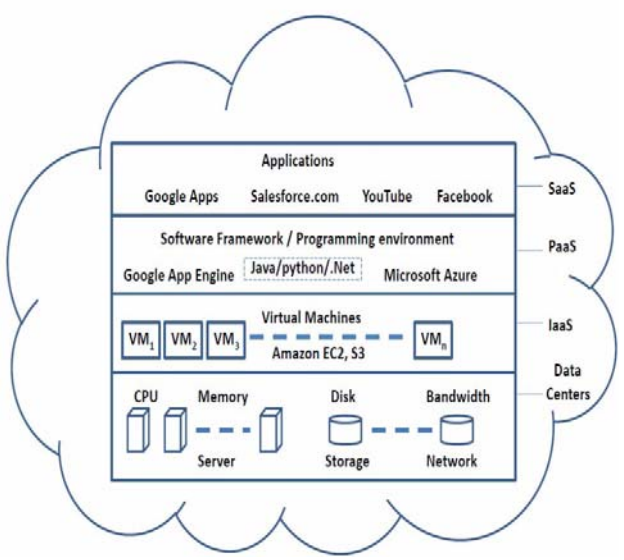

Figure 1. High Level View of Cloud Computing Architecture

Based on this understanding of the term 'cloud computing', there are three major elements or delivery mechanisms for cloud computing[1]:

I. *Infrastructure as a Service (IaaS) or Hardware cloud*

Under the IaaS model, instead of purchasing large and costly infrastructure such as data center, virtual servers, network infrastructure, equipment, etc, users, generally large organizations, source the same as a service from third party service providers. The payment mechanism under this model is 'pay as you use'. The hardware cloud infrastructure allows users to expand as well as contract their requirements based on their business needs. Example: Amazon Web Services, EC2, Gogrid.

II. *Software as a Service (SaaS) or Software cloud*

A software cloud is a specialized software that runs on the hardware cloud. Under this model the service provider hosts several software applications for users to use the software as and when required thereby eliminating the need to install and run the software application on the user's computer and also simplify maintenance and support expenses. This service is in the form of web services and is made available to users over a network which is normally through the web/Internet. Because the service provider hosts both the application and the data, the user is free to use the service from anywhere. Example, GoogleDocs, Salesforce.

III. *Platform as a Service (PaaS) or Desktop cloud*

With PaaS, software developers can avail the platform services to develop various applications without installing and maintaining any tools on their computer. PaaS tools are hosted on service provider's IaaS. Once developed, these applications can be then be tested and deployed without much trouble and effort. Example, Facebook, GoogleApps, Ning, 10gen.

2. CHALLENGES AND LEGAL ISSUES INVOLVED IN CLOUD

Legal Issues

Every new technology brings lots of advantages along with it, and cloud computing is not an exception to it. However it has some grey areas also which needs to be answered. The wide use of cloud computing over the past few years has raised several issues. It must be understand that the purpose of cloud computing service is to facilitate the computing needs of hundreds and thousands organizations over a virtual computing infrastructure located somewhere on the Internet, which is very much contradictory to the conventional service providers. Thus it becomes important on the part of the organizations to get assurance that their data shall be safe, and secure. Apart from these there are some technical and legal issues also.

Data Privacy

The data privacy [5,6] is also one of the key concerns for Cloud computing. A privacy steering committee should also be created to help make decisions related to data privacy. Requirement: This will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators. Data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. Organizations stand a risk of not complying with government policies as would be explained further while the cloud vendors who expose sensitive information risk legal liability. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its own potential risks.

Data security[4,5,6]

If they address the issue at all, vendor form contracts are likely to promise to provide only "reasonable" security for your data, or perhaps to adhere to "industry standard" security practices. While such promises sound good in the abstract, they are open to considerable interpretation and argument. It is preferable to specify an actual, specific, independent security standard and require that it be updated, and perhaps audited, regularly. In addition, for certain kinds of data (e.g., data subject to HIPAA, Gramm-Leach-Bliley, PCI DSS, or the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth), there may be specific security requirements that must be included in any vendor contracts. Ideally, the contract should also provide for regular SAS 70, Type II audits, with customer access to the results.

Finally, the contract should require the vendor to give us notice of any security/data breaches, and, to the extent that user notification is legally required, such notice should preferably be in advance of user notification (which should be the vendor's responsibility).

Access to data for purposes of e-discovery[4,6]

Although the contract probably will not (and probably need not) expressly address the issue, it is important to understand—ahead of time—the architecture of the vendor's system, how and in what format it keeps your data, and what tools are available to you to access your data so that you will be ready for any e-discovery needs that may arise. "Free" services typically will have few such tools available, which likely will make e-discovery a time-consuming and cumbersome task.

Location of data[4,6]

Some vendor form contracts expressly reserve the right to store customer data in any country in which they do business. Others may not address the issue, but the vendors may follow similar practices nevertheless, on the (generally legitimate) theory that what is not expressly prohibited is thereby permitted. While dispersed geographical storage is beneficial from a data protection and backup perspective, it can raise export control (EAR/ITAR) issues in the context of research data. If that is important to you, you should be sure to include language prohibiting "extraterritorial" storage.

Responsibility for end users [1,4]

Vendor form contracts sometimes require us to "ensure" that any end users comply with the vendor's AUP, terms of service, or similar provisions, or (better, though still problematic) to use "best efforts" or "commercially reasonable" efforts to do so. That may be appropriate with respect to faculty and staff, for whom we can be vicariously liable, but it is preferable to provide simply that we will "inform" our students, for whom we are not vicariously liable and over whom we have little control, of their obligation to do so. An alternative, and better yet, would be to provide that the vendor may require student end users to agree directly with the vendor to comply with any such provisions.

Unauthorized or inappropriate use[1,[4]

Vendor form contracts may attempt to make us responsible for affirmatively preventing any "unauthorized" or "inappropriate" use of the vendor's service by others, or perhaps to use "best efforts" or "commercially reasonable efforts" to do so. Given that these services are "in the cloud" and therefore largely outside our control, it is preferable to provide only that we will not "authorize" or "knowingly allow" such uses. Such contracts also may require us to notify the vendor of "all" unauthorized or inappropriate uses of which we become aware. Particularly with respect to vendors with broadly stated AUPs or terms of service, such expansive obligations seem burdensome and unnecessary. It is preferable to replace "all" with "material" or some similar, higher threshold.

Suspension of end user Accounts[1,4]

E-mail services in particular may wish to retain the right to suspend your end users for violations of the vendor's AUP or terms of service. If, as is common, those provisions are broadly stated, the vendor will have almost open-ended authority to suspend your users. It is preferable to limit any such power to a more restrictive standard—perhaps only "material" violations, or violations that "significantly" threaten the security or integrity of the vendor's system.

Emergency security Issues[2,4,9]

Vendors understandably may wish to have the right to "immediately" suspend an "offending use," and possibly the service altogether, in the event of an "emergency" issue. However, the standard for what constitutes an emergency should be clearly defined, should not give the vendor much if any discretion or flexibility in its application, and, preferably, should incorporate a "materiality" or similar threshold.

Suspension and termination of the service[4,9]

Vendor form contracts typically give the vendor the right to suspend the service or to terminate it altogether upon certain events or conditions. Such provisions are not unreasonable in the abstract, but they should be limited in scope to only truly significant matters, provide for an opportunity for you to cure the alleged violations or some form of escalation rather than instantaneous implementation (except in the case of true emergencies), and give you adequate time to make alternative arrangements for your data or service. (In the case of an e-mail system, it may take 6 months or more to establish and transition to a new system, particularly if you intend to completely dismantle your internal system once you outsource.) It also will be important to have assurance your data will continue to be available to you, in a usable format, for at least that long (or, if the vendor is unwilling to commit to a specific length, a "commercially reasonable" period of time) following any termination, as well as that the vendor will return or destroy any copies of your data once transition is complete.

Ownership of data[4,6]
The contract should expressly make clear that all data belongs to the institution (and/or its users) and that the vendor acquires no rights or licenses, including without limitation intellectual property rights or licenses, to use the data for its own purposes by virtue of the transaction. It also may be useful to provide that the vendor does not acquire and may not
claim any security interest in your data.

Publicity [4]
Vendor form contracts sometimes grant the vendor the right to use customer names, logos, and trademarks for purposes of the vendor's own publicity. If such provisions (which are of no benefit to us) cannot be stricken altogether, they should be modified to require prior review and approval (perhaps "which may not unreasonably be withheld"), or at least limit use to the inclusion of our names (but not logos or trademarks) on a customer list, in a manner that does not state or imply an endorsement.

Service level Agreements[4,8,9]
The amount of guaranteed "uptime," the process and timeline for dealing with "downtime," and the consequences for any failures to meet those requirements should be spelled out clearly. In the context of a "free" service, additional "free" service is of no great benefit to us, and no great disincentive to the vendor.

Disclaimer of Warranty[4,8,9]
Vendor form contracts typically disclaim essentially all warranties, sometimes expressly including any warranty that the vendor's service does not infringe third-party intellectualproperty rights. At a minimum, the contract should warrant that the service conforms to and will perform in accordance with its specifications (which should themselves be as detailed as possible, to avoid misunderstandings and disagreements) and that it does *not* infringe any third-party intellectual property rights. Without those two warranties, there is no enforceable assurance that the service will in fact do what the vendor's marketing people claim it will do or that the vendor even has the right to provide it to us—and, if it doesn't work, or if we are sued for infringement, we will have no recourse against the vendor.

Indemnification by Customer[1,4,8,9]
Some vendor form contracts require us to indemnify the vendor not only for our own actions (which is not necessarily unreasonable), but also those of our end users, including students for whom we are not otherwise vicariously liable. With respect to liability for student e-mail, online postings, and the like, this is largely an issue of who will pay the vendor's attorney fees, as the vendor has good legal defenses against claims based on end-user content or actions. Moreover, this is not really taking on a new liability, as we currently can be sued for such content or actions (and have the same legal defenses) as ISPs ourselves. Nevertheless, it is preferable not to voluntarily accept that liability, which is also no different that the vendor's liability for any other, noninstitutional end users. Public institutions may also have significant state-law restrictions on their ability to indemnify.

Indemnification by Vendor[4,8,9]
Vendor form contracts rarely include any form of indemnification benefitting us, but such protection is critical in at least two areas: infringement of third-party intellectual property rights and inappropriate disclosure or data breach, both of which are largely, if not entirely, in the vendor's sole control, and both of which can be extremely costly to defend and remedy. (If, as has happened, a vendor refuses to accept liability for either of these issues on the ground that it's a "black hole," we should take that as a great warning about the vendor's lack of confidence in its own service and look elsewhere—what the vendor is really saying is that it expects *us* to be its insurance company.) Ideally, the vendor would indemnify us for all of its acts and omissions.

Modifications to the Contract[4,8,9]
Vendor form contracts sometimes reserve the right for the vendor to make modifications to its services unilaterally. While some form of right to make changes probably is necessary and appropriate—we certainly would have no objection to improvements—such language is overbroad and does not provide the customer with any assurance that any such modifications will be beneficial, let alone acceptable. Limiting the vendor's right to "commercially reasonable modifications" would be an improvement, but, in the context of a "free" service, could still be expansive. Even better would be to add to that a qualification prohibiting "materially detrimental" modifications—perhaps something to the effect of "Vendor may make commercially reasonable modifications to the Service, provided that they do not materially diminish the nature, scope, or quality of the Service."

Incorporation of URL terms[4]
Similarly, vendor form contracts may incorporate by reference additional terms and policies posted to the vendor's website, which typically are subject to the vendor's unilateral amendment, and those terms and policies may in turn incorporate by reference still other terms and policies posted elsewhere on the vendor's websites, which also typically are subject to the vendor's unilateral amendment. The result is that the contract itself is incomplete, it may well contain provisions that are inconsistent or that conflict with the incorporated provisions, and it likely will be difficult or impossible to fully comprehend. It also will potentially be meaningless, because the vendor will have the right to amend it significantly at any time, and likely even without any more notice to us than posting the change to its website. While it may be reasonable to deal with technical standards and guidelines or other "non-legal" matters elsewhere, it is strongly preferable that all contractual terms be included in the contract itself. At the very least, the customer should attempt to require the vendor to provide direct, individual notice sufficiently in advance of the effective date of any

amendments to incorporated terms, along with the right to terminate if such amendments are unacceptable or materially detrimental to the customer's interests.

Automatic renewal [4,8,9]

Vendor form contracts typically renew automatically for additional terms unless we give specified prior notice. This is probably not a major concern in the context of "free" services, assuming there is nothing in the contract that actually requires us to use the service (particularly exclusively); we can simply cease to use it, with no significant adverse consequence. In other cases, however, it will be important to use a "tickler" system to remind us when we need to make a decision about renewal and give notice of any termination. Ideally, the contract would renew automatically (so we don't have to renegotiate every time), but also allow termination for convenience on some reasonably short period of notice.

Governing law and Jurisdiction[4,8,9]

Almost certainly, a vendor's form contract will specify that it is governed by the law of the vendor's home state and grant the courts of that state exclusive jurisdiction over any disputes arising out of the contract. Public institutions generally have significant state-law restrictions on their ability to consent to such provisions, and they are inadvisable for others. It is preferable to either (a) specify the law and jurisdiction of our own state (large vendors likely operate in and are subject to all such jurisdictions, so it is no significant inconvenience for them), (b) provide that disputes must be brought in the defendant's jurisdiction (which is even-handed and tends to encourage informal resolution, as the plaintiff won't have the "home court" advantage), or (c) simply delete the provision and leave the question open for later argument and resolution if and when needed.

CONCLUSION

In cloud data storage allocation is done through infrastructure, as at different level through national boundaries laws and jurisdiction varies. Every time the challenges may be same but laws are different, through this paper we are going to discuss about various challenge for cloud and discussing about legality of transmission location and manageability of the data.

As the Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits their security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offered are immature or inexistent. We have presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. As described in this paper, data storage, data privacy , and networks are the biggest security concerns in Cloud Computing.

REFERENCES

[1] Nishith Desai Associates,' Cloud Computing Risks/Challenges-Legal & Tax Issues' in March 2013,PP.1-26.

[2] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy,' Cloud Computing: Security Issues and Research Challenges' in IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 1, No. 2, December 2011,PP.136-146.

[3] G A Solanki ,' Welcome To The Future of Computing: Cloud' in INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 1, ISSUE 9, OCTOBER 2012, PP.30-34.

[4] Steve McDonald, General Counsel, Rhode Island School of Design,' Legal and Quasi-Legal Issues in Cloud Computing Contracts' PP.1-4.

[5] Ronald L. Krutz, Russell Dean Vines "Cloud SecurityA Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, Inc.,2010.

[6] Puneet Kumar and Harwant Singh Arri ," Data Location in Cloud Computing" in International Journal for Science and Emerging Technologies with Latest Trends" 5(1): 24-27 (2013).

[7] MITCHELL COCHRAN," GOVERNANCE AND SERVICE LEVEL AGREEMENT ISSUES IN A CLOUD COMPUTING ENVIRONMENT" in Journal of Information Technology Management, Volume XXII, Number 2, 2011,PP.41-55.

[8] S.B.Dash, H.Saini , T.C.Panda, A. Mishra ," Service Level Agreement Assurance in Cloud Computing: A Trust Issue"in (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 2899-2906.

[9] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez," An analysis of security issues for cloud computing" in Journal of Internet Services and Applications (Springer) 2013,PP. 1-13.