IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

A Study On Cloud Computing And Cloud Contracts Negotiation

Adv. Shriya .J. Sayanak
LLM Student
Christ University

Abstract

Cloud computing is a technology that allows users to access computing resources from a remote location. The relationship between the cloud provider, customer and end-user may determine the cloud computing contracts. In this research paper, we will see the working and storage of cloud computing services. Cloud contracts are usually non-negotiable, and the cloud providers fix the jurisdiction. In this research paper, we will see how the cloud providers have a limited or no liability principle in breach cases. This paper will also see if there can be negotiations in clickwrap contracts and, if so, how the negotiations work. With the new rules of data access in different countries, the data location becomes crucial for the customer to choose the type of cloud and the country where the server is located, depending upon the confidentiality and integrity of data. The cloud migration and data fragmentation rules and regulations and difficulties concerning cloud migration data Fragmentation and data storage are also discussed in this paper.

Keywords: cloud computing, cloud deployment models, cloud service models, cloud contracts, cloud contract negotiation, Cloudbusting, cloud migration

What is cloud computing?

To understand the basics of computing, we must first see the definitions of provider, customer, and end user. A provider is a person who provides cloud computing services. A customer is a person who has a contract with the cloud provider, and the end user is an individual who uses the cloud services. Therefore, a cloud computing service when convenient on-demand network access is used in a shared pool of configured computing resources that can rapidly be provisioned and released with minimum management and effort or service provider interaction.[1] The cloud computing service, in simple terms, is remote access of servers, storage, space and software applications through the Internet to computer resources on demand. Almost everyone in today's world uses cloud services. Basic Gmail uses the Google Cloud, social media platforms like Facebook, Instagram and streaming platforms like Netflix, Amazon Prime, etc. Use some of the other kinds of cloud

How does the computing system work?

The primary computing system has three components that are hardware, logical layers and content layer. Hardware is the things that we can see, like desktops, cables, et cetera. The logical layer is the internal software used to run the computer. The logical layer contains operating software and software applications, and the content layer has the content that the user stores. To get the content, a combination of hardware and logical layers is used. Initially, the content used to be stored in the computer hardware only. But now, with the Internet, the information can be

[1] Jatinder Singh , C. Millard, W. kaun . Hon. "Cloud Computing Demystified (Part2) Control, Security and Risk in Cloud." In *Cloud Computing Law*, 2nd ed., 2022.

stored remotely on a service called cloud computing

Why do we use cloud computing?

Cloud computing is used because it is cost-effective. The amount of hardware to be Brought to store massive data will cost the user—a lot of money. If cloud computing is used the user may get storage with less money. Cloud computing is flexible meaning that the availability of data can be from anywhere at any time. In the case of traditional hardware storage of data the customer had to use the particular hardware to access data but now due to cloud computing and the Internet, the data can be accessed from anywhere. scalability of storage storage of data is also easy in cloud computing. The specialization of cloud computing has also become easier these days. No, there are some advantages like trust issues, control and security issues. The user would get more benefits by using cloud computing.

What is Cloud migration?

Cloud migration is a process of moving to the cloud computing services from a established and legalized IT system. In simple words, cloud migration means to store the traditional hardware data from the IT system to the cloud system. There are many cultural and legal concerns that come with cloud migration.the cultural obstacles being that the cloud might jeopardize the jobs of many IT departments and that it would become expensive to migrate to cloud. The legal regulations can range from cross-border data to sector specific concerns[2].

Where is data stored in cloud ?

In the conventional hardware, IT storage,The data is broken down into small blocks and stored in the operating operating system and whenever we want to access it, the operating system resembles the required data and we can access it. In case of cloud computing, digital file is stored on providers cloud server. Fragments of data are stored on different computing servers. This is called data fragmentation or data shredding. Depending upon the type of data, duration of data to be stored, cost of storage, the data can be stored in different servers.

This may attract a lot of legal implications, depending on the laws relating to the international data transfers, foreign government has different laws for access of data. Therefore, now the customer can select the location of the data storage.

The customers concerns with data location are the data protection laws that are prevalent in the country in which the servers are located. There are certain countries in which the government can access the data from the cloud computing servers. In case of such access by authorised user or without intimation to the authorised User, the law enforcement applicable would also change and would also Mean that the customer has to be very careful. The data localisation laws very across the nations and this could lead to loss for the customer.

Nowadays, while negotiating the terms and conditions of the cloud computing contracts, the customers have the option of choosing the data location for some cases. However, while tailoring the location of data, the customer usually has to pay an extra price to choose the location.

What are the types of cloud services?

The cloud services can basically be divided into three types namely

1. Infrastructure as a service (IaaS)
2. Platform as a service (PaaS)
3. Software as a service(SaaS)

In infrastructure as a service, the provider manages the hardware such as the cloud service as well as the software that creates and separates virtual machines. The customer has control over these machines and can install software to use the machine.

In case of platform as a service the provider manages hardware and provides framework for developing and deploying new software. Customer can use this to build and deploy software applications.PaaS gives less control to the customer

In case of software as a service, the provider manages the hardware and runs the software application on the cloud. The customer only access via the Internet and install on a local Drive. In this the customer has access over only

[2] Jatinder Singh , C. Millard, W. kaun . Hon. “Cloud Computing Demystified (Part2) Control, Security and Risk in Cloud.” In *Cloud Computing Law*, 2nd ed., 2022.

the data and input the provider manages rest all things.

What are the types of cloud deployment methods?
Cloud deployment model are of 3 types they are

- Public cloud
- Private cloud
- Hybrid cloud
- Multi cloud

Public cloud where multiple customers or tenants share access to the same underlying hardware. The public cloud servers are mostly located in the choice of place decided by provider. The provider separates different customers by using software logic layer.basically the provider uses logical separation to separate between the users of public cloud. Private cloud has separate resources at hardware level by using physical separate servers. Sometimes the user may ask for the Installation of servers in the personal area or the personal space also. The private cloud may install the servers of premises on the premise of the user. The private cloud user may also use the internal private cloud which is on the premise of the provider itself. The private cloud is usually more expensive and takes longer to deploy. Although the private cloud is more expensive due to the physical separation, the private cloud tends to be more secure. In The public cloud multiple people use the same servers. Therefore, there is a chance of leakage of privacy or data leak.on public cloud. If anyone person miss uses, then the entire server can be brought down. In case of private cloud the risk streaming from other customers is lower and also there is physical security. Hybrid crowd is a combination of different cloud deployment methods. cloud bursting means use of private cloud for some work and public cloud for some work. During Cloudbusting, the scaling up of use of public cloud can be done for load balancing. multi cloud system is when single customers uses multiple clouds for example, a single customer may use Gmail, dropbox, Adobe et cetera
This is important because depending upon the type of deployment method, it can raise different legal implications with regard to cloud computing.

Cloud laying can be when one cloud is built on the top of another. For example, in case of Netflix the software as an service and infrastructure as a service have been layered together to form the end product.

Is cloud computing secure?
Security in cloud computing can be divided into confidentiality, integrity and availability of data. For a cloud computing system to be secure, it has to have all the three factors of security. In case of confidentiality, the user must be assured that the access of data is only authorised by the User. The data cannot be allowed to access by any other person other than the authorised user. further the user has to be assured that any changes in data can only be done by the authorised user. This is called integrity of data and the third factor for security in computing service is the axis of data has to be only by the authorised user and has to be available at the convenience of the user. sometimes it’s so happens that the availability of data becomes difficult and thus the security can be hampered.
Threat is defined as a set of circumstances that would lead to vulnerability being exploited. Threat is when the risk management and risk assessment of data goes for a toss.

Cyber security and cloud computing.
The laws require the providers to asses the risk and put in place appropriate risk management techniques in order to ensure security of the data. risk is when the cloud is access to the Internet by some other person just can also be when the network is down and the data cannot be accessed by the user at appropriate time. Also risk can be when Theresa delayed during the data transfer, which is called as latency of data. of public cloud, the risk is higher because the server is accessed by multiple people at the same time and a hacker can easily access the data[3]

The security in cloud computing is managed depending upon the type of cloud that is being used. in case of infrastructure as a surface, the provider has control over the hardware. Physical security and logical separation is managed by the provider. The customer has to manage the security of the remaining layer in case of platform. As

[3] John David Michaels, Christopher Millard, Felicity Turton. “Contracts for Clouds, Revisited: An Analysis of the Standard Contracts for 40 Cloud Computing Services.” *QMUL Cloud Legal Project*, n.d.

a service, the provider has more control. Customer can have application level security installed. In case of software as a service control of all the layers is at the providers end customers need not worry about the security.

What are cloud contracts?

We have studied that for any contract to be valid, It has to have a offer, acceptance, consideration and intention to contract.

Cloud computing contracts are online contracts. The cloud contracts have a set of terms of services and by clicking the " I agree" the contract is term to be accepted. These type of contracts are called clickwrap contracts. The cloud contracts are usually the click wrap contracts.

The cloud contract has terms of services ToS , privacy policy, data processing addendum, acceptable usage policy, and law enforcement guidelines[4]. The customers of cloud do not usually read such huge contracts. According to the English law, if a party sign the contract, they will be bound by the contract. Cloud customers usually do not get a chance of negotiating with the providers because the terms and contract are uniform for better efficiency and legal certainty.

Is negotiation possible in cloud contracts?

Negotiation is usually not possible in cloud contracts because cloud providers do not negotiate with the customers. The cloud providers have a basic uniform terms of services applicable to all the customers. The cloud providers have commodity pricing where the fixed price is allowed for the services of cloud computing. The cloud providers say that these kind of contracts which are uniform in nature and have commodity pricing are more efficient. The legal certainty of these contracts is also higher than the negotiated kind of contract.

The cloud contract is on one too many basis. This means that there are standard contract terms called as terms of service. Usually a cloud contracts on a ticket or leave it basis. However, for certain large customers there is scope of negotiation. in case the customer has a business of more than £1 billion, Then there is 70% chances of negotiation. in case the customer has a business of less than £500,000. Then there is only 30% chances of negotiation. Therefore the scope of negotiation depends on the size of the business that the customers have.[5]

The main factors while considering negotiation between the customers and the providers are predicted, annual revenue or overall IT budget and strategic advancement.

The customers mainly negotiate the following terms

1. Internal reasons for negotiation

In this, the commercial considerations are taken into scope and price, risk locations and security requirements are negotiated

2. External reasons for negotiations

In this regulation and insurance is mainly negotiated

The top five terms that are negotiated can be data breach-response and liability, limitation of liability, data, ownership, and usage rights, indemnification and data, security and redundancy

What is the jurisdiction of cloud computing contracts?

Over 80% of the cloud computing contracts have exclusive jurisdiction clause. The jurisdiction to try the case has to be in accordance with the choice of law clause mentioned mentioned in the cloud computing contracts. The most popular choice of law is the English law and the English courts. The jurisdiction of the cloud contract is usually mentioned in the contract itself. the choice of law clause is present in the contract which will give the guidelines of the law that would be applicable in case of breach by any party. In the European Union, private international law is applicable in case of cloud contract breach. The Rome I regulation is usually applicable for such contracts. This law is applicable in the UK as well even after the present.

The choice of law clause usually contains the choice of law that is the jurisdiction which is binding on both the parties. The freedom of contract is present in the class, which states that in case of default, the case can be filed

[4] Christopher Millard, W Kuan Hon. "Use by Banks of Cloud Computing: An Empirical Study." *QMUL Cloud Legal Project*, 2016.

[5] W Kaum Hon, Christopher Millerard, Ian Walden. "Negotiating Cloud Contracts: Looking at Cloud from Both the Sides." *Stanford Tech Technology, Law Review* 16, no. 1 (2012).

with the service provider resides. The service contracts are governed by the providers law.

In cases where the consumer is to be cheated or where consumer protection law applicable the case can be filed in the place where the person recites. However, consumer protection is applicable only to the individual persons and not to the companies who use cloud computing.

Under the Rome I regulation, if there is no choice, then the contract may be governed by the law of the country in which the service provider is located. Most of the cloud computing contracts have a choice of law clause and the popular choice for the law is the European law.

There are certain cloud computing contracts in which there is arbitration that is made mandatory in the contract itself. in case the contract makes the arbitration compulsory, Then the parties have to abide by it and go for arbitration only and cannot file a suit in front of the courts. However, there is an exception for the consumer where in case of breach the consumer can apply consumer protection law and go to the quotes instead of arbitration[6].

What are the remedies available in case of breach?

In cases of breach, the remedies available are termination, claiming of damages and specific performance. The agreived party can ask for specific performance of certain duties that match the contract. The aggrieved party may ask for termination of the entire contract or claim damages in the form of monetary compensation. The damages have to be claimed for foreseeable breach.

The cloud providers have to give services with a certain duty and care. According to English law, the duty of the provider to give service with reasonable care is an implied clause in the contract reasonable care and skill has to be there on the behalf of provider. However this clause can be changed if there is an express terms mentioned in the Cloud contract

In reality…,

If the customer is at laws, the only option available to the customer is to stop the use and terminate the contract. The providers usually have a broad exclusion of liability. The providers make sure that they exclude all damages and cap the liability. In case of business to business transactions(B2B) , there can be some limited liability that can be placed on the provider. Example Apple iCloud has provider liability which is limited and there is a cap on liability. Consumer may so the Apple iCloud in cases of failure to use reasonable care, gross negligence by the provider and willful misconduct.

In service level agreements, there is a level of service that is to be provided by the provider. This is a measurable criteria and fixed compensation can be claimed in cases of cloud computing for service level agreements. In case of cloud service level agreement. Usually a monthly uptime percentage is provided as liability by the provider.

Can liability be limited under the English law?

Liability can be limited under English law in certain cases. However, this can be challenged in front of the court. The rule of reasonableness is applied by limiting the liability. Case by case assessment is done by the court while deciding the limitation on liability. However, freedom to has to be there while deciding this[7].

Can cloud contracts be terminated?

Usually when we are talking about the cloud contracts, they run for infinite number of years. However, the customers can choose to terminate the contract at any time. Once the contract is terminated cloud migration is pretty difficult on part of the customer.

In case the provider decides to terminate the contract, he can do it at any time and for any reason. The provider has sold discretion for terminating the contract. There are specified listed terms which the contractors have to follow. In case of termination, the specified listed terms can be breach of contract, breach of AUP (acceptable

[6] W Kaum Hon, Christopher Millerard, Ian Walden. "Negotiating Cloud Contracts: Looking at Cloud from Both the Sides." *Stanford Tech Technology, Law Review* 16, no. 1 (2012).

[7] John David Michaels, Christopher Millard, Felicity Turton. "Contracts for Clouds, Revisited: An Analysis of the Standard Contracts for 40 Cloud Computing Services." *QMUL Cloud Legal Project*, n.d.

usage policy), or suspension or termination[8].

After the termination by the provider, it becomes very difficult for the customer to retrieve data. Contracts may differ with regard to post termination arrangement. Some cloud providers completely delete the data post termination. in some cases, a grace period is provided by the provider for retrieval of the data post which the data is deleted permanently.

Can security be negotiated?

The security for data can also be negotiated in the negotiation phase , between the customers and providers. The customer may ask for security certificates of the cloud computing company. SOC2 audit reports can be asked by the customer or the customer may demand for a security ordered by an independent expert in order to reassure the security provisions.

There are various testing also done by the customer in order to reassure the security[9]. The testing can be

1. Pen testing or penetration test

In this type of testing, the customer may hire someone from the outside to breach the security of the providers servers. this is done by the permission of the provider. This is done to reassure the customers of the security which is provided by the cloud computing company. This is confined to sandbox and certain this is done by the permission of the provider. This is done to reassure the customers of the security which is provided by the cloud computing company. This is confined to sandbox and certain times only.

2. Breach notification

In breach notification, it is to notify the security incidents to be the customer. it is a regulatory requirement that has to be followed by the providers of cloud computing company. There is a specific time frame and a method that has to be followed by the company while doing this kind of test. this is used to notify the incidence to the customer.

3. Breach liability

In case of breach liability, some providers except liability and some don’t, there are higher caps for damages in case of breach[10]

Can audit right been negotiated ?

In case of negotiation of audit rights, the customer has the right to inspect the providers operating operating system. The negotiation of audit rights can be done by inspection of premises and devices. The providers are required to reveal all the sensitive information in order to analyse the risk. This is usually done in cases of public cloud where the security is a little weak in cases of using a server for many people.

Conclusion and suggestion

While negotiating and deciding the jurisdiction for the cloud computing contracts, the customer has very limited scope. The providers make sure that the liability that can be put on the provider is limited or not there at all. This puts the customer in a weaker position as the cloud contacts are on, take it or leave it basis. With the growing popularity of cloud computing, the cloud providers have to take into consideration the customers requirements and modify their cloud contracts according to the requirement of the customers. Today we can see that the cloud contracts are usually negotiated only for big players but it would be great if some term and conditions could be altered and adjusted according to the requirements of the individual customers as well. In the future, we might be able to see the cloud contacts to be altered according to the needs of the customer.

[8] W Kaum Hon, Christopher Millerard, Ian Walden. “Negotiating Cloud Contracts: Looking at Cloud from Both the Sides.” *Stanford Tech Technology, Law Review* 16, no. 1 (2012).

[9] W Kaum Hon, Christopher Millerard, Ian Walden. “Negotiating Cloud Contracts: Looking at Cloud from Both the Sides.” *Stanford Tech Technology, Law Review* 16, no. 1 (2012).

[10] Christopher Millard, W Kuan Hon. “Use by Banks of Cloud Computing: An Empirical Study.” *QMUL Cloud Legal Project*, 2016.

REFERENCES

1. Jatinder Singh , C. Millard, W. kaun . Hon. “Cloud Computing Demystified (Part2) Control, Security and Risk in Cloud.” In Cloud Computing Law, 2nd ed., 2022.
2. W Kaum Hon, Christopher Millerard, Ian Walden. “Negotiating Cloud Contracts: Looking at Cloud from Both the Sides.” Stanford Tech Technology, Law Review 16, no. 1 (2012).
3. Christopher Millard, W Kuan Hon. “Use by Banks of Cloud Computing: An Empirical Study.” QMUL Cloud Legal Project, 2016.
4. John David Michaels, Christopher Millard, Felicity Turton. “Contracts for Clouds, Revisited: An Analysis of the Standard Contracts for 40 Cloud Computing Services.” QMUL Cloud Legal Project, n.d.
5. Chris Reed. “Information Ownership in Cloud.” In Cloud Computing Law, 2nd ed., 2022.