Contracts in Cloud Computing

Irene Kafeza

National Academy of Legal Studies Research (NALSAR)

Hyderaband, India
kafeza@nalsar.ac.in

Eleanna Kafeza
Business School, Dept. Marketing and Communication
Athens University of Economics and Business Athens, Greece
kafeza@aueb.gr

Epameinondas Panas School of Science and TechnologyDept. of Statistics

Athens University of Economics and Business
panas@aueb.gr

***Abstract*— In an increasingly integrated global economy the importance as well as the growing availability of Cloud Providers has provided companies, individuals and the Governmental agencies with a variety of benefits such as significant cost reduction. As the role and number of Cloud Providers has increased a novel set of issues has emerged. These novel issues refer to a variety of legal complexities from the initial choice of the proper Cloud Provider as well as the appropriate contract for the deployment of its services.**

This paper is concerned with the novel issues arising of the deployment of Cloud Computing contracts. It presents the related issues and discusses ways and suggestions by which the legal framework could be demystified so that the contracts conducted in the Cloud Computing environment can be conducted efficiently and in a legal manner, for the benefit of the private as well as the public sector. It is concerned that the current legal framework cannot provide solution for effective deployment of Cloud Computing contracts and drawing on this evidence, it discusses the steps that Cloud Computing participants need to take to correctly identify their contractual rights and obligations.

Keywords—legal issues; cloud contracting; SLA contracts;

I. INTRODUCTION

Cloud Computing services meet the worldwide business demand for intense problem solving capabilities and makes it possible to share Computing resources on an unprecedented scale among geographically distributed participants. The Cloud Provider allows the dynamic discovery of Computing resources, the immediate allocation and provision of the resources, as well as the management and provision of secure access to those resources. This redefinition of allocation and distribution of services arises as an emerging Computing paradigm and is expected to change the IT landscape including technology, business and services.

Cloud Computing environment refers to a collection of heterogeneous Computing resources that are shared by many individuals and organizations.These resources are collaborating collaborating to offer more effective solutions to a variety of business problems. A successful Cloud business model requires a secure platform that will enable safe and stable collaboration of various resource owners and service users. This requirement is twofold: on one hand a secure technical infrastructure has to be in place and on the other hand a legal framework has to be introduced to increase confidentiality and enable predictability of commercial transactions on the cloud. From the legal point of view several issues have to be addressed in order to create a trusted Cloud environment for business transaction

Cloud Computing has been viewed as an opportunity for faster, better and cheaper services. It has lower costs for storage and computing, is quick and cheap to setup, and allows for flexibility by making applications available at remote offices, on the road, via a smartphone, or from a home PC. It is expected that in the future a typical workplace will include several Cloud Computing applications. An important feature of this service is that all issues regarding the update of software licenses, software updates, hardware failure, adding of capacity are resolved by the SaaS Cloud provider. However, cloud computing deployment raises some concerns such as how can the user trust the Provider that the service will be always available or whether the Provider can be trusted with sensitive data. Private and public sector organizations when entering into a Cloud Provider agreement for rendering its services must be sure that the Cloud Computing function is in compliance with the legislation. Most importantly the user needs to know his rights and obligations as well as the Cloud provider's rights and obligations towards him.

The existing Cloud computing environment lacks a legal framework that allows safe transactions among the organizations that dynamically form the cloud. At the same time, the way contracts can be created and managed in a Cloud Computing environment is of paramount importance for planning and implementing clouds.

II. CLOUD COMPUTING CONTRACTS

A. Cloud computing non-negotiated contracts

1) Background

The core issue in the adoption of Cloud Computing services is related to the adoption of the proper contractual model for the Cloud services. Selecting the right Cloud service Provider is the first critical step towards the Cloud Computing adoption. Depending on the user's needs the Saas or Pass or IaaS type of Cloud Computing will be selected. The choice of the appropriate service is vital for the specific purpose for which users employ the Cloud environment. After the selection of the right service, the user needs to enter into a contract with the selected Cloud service provider. This contract can be either a negotiable contract or a standard form contract.

There is different terminology used for Cloud computing contracts. Other companies use the term "Master agreement" for the main agreement with the cloud user and "Service Level Agreement "for the separate contract that regulates the specification of the services. Other companies use the term "Terms of Use" for the general contract and other companies use the "Term of Use "for the general contract that incorporates the Service Level Agreement. For the purpose of this work the terminology "terms of use" or "Cloud Provider contract" means the main contract which incorporates the Service Level Agreement. Therefore, in this work, the Cloud Provider Contract refers to the general clauses of the contract with the Service Provider as well as includes the Service Level Agreements (SLA) which refers to the terms for the specification of services e.g. scalability etc.

There is not a uniformly accepted definition of what constitutes contract. Contract is a promise or a set of promises for the breach of which the law gives a remedy or the performance of which the law in some way recognizes as a duty [1]. An agreement enforceable by law is a contract [2].

An electronic contract extends these definitions to electronic agreements; agreements created through electronic means. These agreements can be classified either as negotiable agreements where the parties can negotiate the terms of the contract or standard form agreements in which the contract is drafted by one party and the other party can only "take it or leave it". The standard form agreements (or adhesion contracts or boilerplate contracts or mass market contracts or Terms of Service) appeared when the computer software industry was faced with huge loss of money due to piracy of software. Although the reproduction of software without authorization is prohibited by the Copyright legislation, the IT companies could not efficiently prohibit the unauthorized reproduction.

The main reason was that the enforcement of rights of the copyright owner under the copyright law has been proved difficult and inefficient. Thus, the software companies attempted to enforce their rights through standard form contracts that restricted the user's rights. These contracts initially were the shrink wrap contracts, (where the license is included in a software package that covers the purchased software and can be read only after the buyer of the software opens the plastic wrap of the software), the click wrap contracts(electronic form agreements set up by one party to which the other party may assent by clicking on the "I agree" button) and browse-wrap contracts (binding agreements simply by visiting the site without the need of clicking any button).

2) Cloud computing contracts as click-up contracts

One of the above categories of standard form contracts, the click wrap contracts, is the usual type of contracts that the Cloud Provider and the Cloud user enter into. These contracts are referred to as Cloud provider's contracts or Service Level Agreements. The Cloud Provider either provide the client user with one document to sign that is titled Master Agreement or Service Level Agreement or Terms of Service and incorporates terms regulating the quality of its service 's performance or the Cloud Provider gives two set of contracts to the user to sign. Thus, the first contract refers to the general terms of service (Master Agreement) and the second contract (Service Level Agreement) refers to the quality of Cloud Provider Services.

The Cloud Provider contract incorporating the Service Level Agreement is usually presented on the Cloud Provider's site and the user has to click the acceptance ("I agree") button in order to proceed to the Cloud Provider Contract. These types of contracts are convenient and cost effective for the Cloud Providers since they don't need to bargain individually with each user therefore saving costs for personnel salaries, time etc. However, the main drawback of these types of contracts that have been challenged on the Courts is that they do not comply with the notion of entering into valid contract according to the principles of traditional contract law. Particularly, their enforceability has been challenged on the ground of the inequality of power between the parties since the vendor is the one who drafts the terms in his favour. The Courts in order to come with a justifiable solution to these issues have applied the "assent analysis "test in order to determine the validity of such contract. The "assent analysis" is to examine whether the user has actually clicked the acceptance icon or has proceeded in a manner that would be impossible to proceed without clicking the acceptance button. Thus, if the Court is satisfied that the user has actually accepted the click wrap contract by clicking the "I agree" button, holds the click wrap contract enforceable. The Courts have denied the validity of click wrap contracts only in cases in which the user has not been adequately informed that his assent is needed or his assent was not required in order to proceed to the contract thus, he has not clearly accepted.

For example, in the Microsoft Azure site in order to proceed to Azure you need to click the button that states " I Agree to the Windows Azure Agreement , Offer Details and Privacy Statement" otherwise you cannot sign in. This is a click wrap contract and the user is bound from its term once he clicks" I agree". But to what exactly he is bound? He is bound to the Windows Azure Agreement. To enter this agreement the user needs to click the button, which is in an obvious position on the site, thus adequate notice is there that qualifies as informed consent that leads to a binding contract.

This agreement includes a term that states "Microsoft Azure Agreement consists of the below terms and conditions as well as the SLAs". In order to read the SLAs the user needs to go to the left of the website and click the relevant link that takes them to the SLAs. The question that arises is: is the SLA included in the click wrap contract? According to the Courts decisions, someone may argue that is not since the user needs to go through all these buttons to enter into the Service Level Agreement. This process does not qualify as" informed consent" although the agreement is on the site because the user has to go all these clicks in order to read the SLA. Thus, the user is bound only by the first click wrap agreement which is presented in an obvious manner and request for a clear acceptance while the SLA is not part of the click wrap contract since it is not presented in a clear and obvious manner to the user. The fact that the click wrap agreement mentions that the SLA is included in the contract does not constitute adequate notice which is required for the valid acceptance. Therefore, the Azure user has a contract for the general terms but not a binding contract for the SLA.

3) User's perspective

Moreover, the contracts with the Cloud Service Provider (including the Service Level Agreement) are often long and include terminology that is not easily understood by the user. Sometimes, the terms are not provided in a visible and easy accessible way to the users. Some other times, the users don't have the time to read them. The result is that Cloud users are not sufficiently informed about their rights and obligations when entering into a contract with a Cloud provider. The general principles of contract law apply in these cases where, as discussed above, the Cloud Providers should have clear terms, ask for the affirmative acceptance of the Cloud user as well as the Terms of Use and Service Level Agreement must be presented in an obvious manner to the user before he enters into the contract. Otherwise, the validity of contract is questionable since the assent of the user might not qualify as adequate acceptance resulting in a binding contract. On the other hand, if the Cloud Provider has clear terms, provides adequate notice to the Cloud user and the user accepts, a valid contract is formed.

4) Limitation of Liability and Disclaimers

Although the contract with the Cloud Provider might be valid, it still might contain certain terms that their validity is questionable. Courts have invalidated specific terms on click wrap contracts when the specific terms are extremely onerous for the other party. One set of terms that have been discussed and created controversies are the terms regarding limitations of liability and disclaimers referring to the services rendered.

One of these terms is the limitation of liability clauses. Liability of the Cloud Provider might arise where the Cloud user has suffered damage because he relied to the information provided by the Cloud Provider which was inaccurate or false. These limitations of liability clauses give the right to the Cloud Provider to disclaim its liability usually through disclaimers. These terms exclude liability of the Cloud Provider for non-performance of its services or false performance and a variety of other instances in which the services might not be provided as prescribed in the contract. Considering that he primary function of Cloud Provider is the assurance of the quality of the service, the question that naturally arises is what is the use of using the service since the Provider that provides it and its primary responsibility is to assure its accuracy has disclaimed all responsibility.

The issue of liability refers to a variety of instances where the things might go wrong. Can an exception clause exclude liability for these instances and will the courts accept such clause as valid? Since there is no specific legislation that addresses these issues a question arises whether the Cloud Provider could by itself pose the standards and rules upon which its conduct will be based and state in its Service Level Agreement what obligations and responsibilities is willing to undertake. Moreover, it is doubtful whether the Cloud Provider will be liable only for losses caused from reliance on erroneously performed services or additionally for no-self compliance with its policies. The liability issues associated with these questions are related with the degree of fault and the extent to which the Cloud Provider is able to disclaim or limit his liability. The question is: what is the point of entering into a contract with a Cloud Provider to employ its services if it is not certain whether it is going to provide the requested service and there is not any consequence for this? The Cloud Providers have argued that the provision of service is cheap and thus one cannot expect to have high standard of assurance while paying so low. Cloud Providers argue that if we try to force Providers to accept more liability while asking them to maintain low commodity prices, the result will be Providers to undermine market development [3].

Absent a coherent legal framework the Cloud Provider could by itself pose the standards and rules upon which its conduct will be based and state in its Terms of Use what obligations and responsibilities is willing to undertake. In this case the wording of the contract will determine the contractual obligations of the parties. Therefore, to ensure enforceability the parties should focus on the following issues: Notice and consent: have the parties clearly and explicitly given their informed consent to conduct the transaction? Have adequate notices provided by the Cloud Provider? Have signature formalities required for this transaction been satisfied? Are copies of the Cloud Provider and user contract available to all parties?

Although the limitation of liability clause is an important one, there are a set of other clauses that the Cloud user might not agree upon. The Cloud Contract usually includes a term that the Provider can change the terms without any notification. The user in this case, either might attempt to negotiate the change of this term and include a term that the Cloud Provider should inform him about the changes as well as a term that he has the right to terminate the contract if he does not agree with new terms.

.

5) Liability under Tort Law

Cloud users would be entitled to recover damages against a Cloud Provider for a breach of contract based on reasonable reliance on performance of its services as stated in its Service Level Agreements Additionally, the Cloud user could base his claims against the Cloud Provider on tort law for negligence if he can demonstrate that the Cloud Provider didn't show the care he ought to show for the provision of its services. Since the core business of the Cloud Provider is the provision of professional level of specific services it seems that he should comply with higher standards of professional care This kind of professional liability for negligence apply to persons that are professionals having specialized knowledge and skills so other people put special trust on them due to this specialization, thus the courts apply to them a higher standard of care than of that of a reasonable man. It seems that the Cloud Provider's fall under the definitions of professional duty of care. Nevertheless, it is questionable whether this is a correct approach and whether higher negligence standards would be more suitable to the nature of their businesses to be imposed to them.

Although we employ the traditional doctrines of contract law to deal with these situations still there is uncertainty regarding the obligations and liabilities of Cloud Providers which self- limiting almost any liability of theirs while their role is to provide assurance and trust for the service. The existing legislation is not addressing particularly these issues thus it seems that either a new legislation should be enacted or the burden of solving this complex situation will be on the courts.

B. Cloud Computing negotiated contracts

In other instances the contracts with the Cloud Providers are negotiable and not presented in a standard form. These contracts –incorporating Service Level Agreements or titled as Service Level Agreements) should specify what type of Cloud service will be provided to the customer to ensure that: a) key elements required for Cloud services (warranties, guarantees, performance metrics, etc.) are not left out of the SLA and therefore rendered unenforceable, b) common terms and definitions are used within the SLAs to avoid costly misunderstandings between parties, and c) to create an environment which allows agencies to objectively compare competing services [4]. These contracts can be signed either with the physical presence of the parties or through electronic means. The" Functional Equivalence" approach or "non-discrimination" doctrine which does not deny enforceability of a contract solely on the ground that it is in electronic form is almost universally accepted principle. Thus, a contract with a Cloud Provider might be entered into electronically and it is valid as long as the substantive law requirements are fulfilled including the signing of the parties.

Most common is the conclusion of these contracts through email. AS long as the writing and signing requirements are fulfilled, these are valid contracts. When negotiating these contracts it might be better if parties include clauses clarifying the form of possible later amendment. There is a discussion whether an oral modification clause or email exchanges could amend a contract thus it is advisable to clarify the form of later modifications of these contracts.

1) Challenging the identity of specifications

Moreover, the Cloud user should read carefully all the terms in the Cloud Provider contract. Sometimes, there is a term for free services. Users should be skeptical about the availability of "free" services since there is another term that charges for the "free" services. There are terms that allow the transfer of the user's data in third parties. Users should clarify with the Cloud Provider the meaning of third parties and decide whether they would like to agree on such a term. Sometimes there is term that in busy working hours there would be a downtime. Depending on the user's needs this might be a term that nullifies the usability of the contract.

The renewal term is also important. The term should be clear whether the service would be renewable automatically and what happens if no. For example in case that the term in not renewable what happens with the Cloud users data: will be kept by the Cloud Provider or it will return them to the user.

The Cloud user must check whether there is a term that allows subcontracting of the Cloud Providers services or a term that allows the transfer of control to another Cloud Provider. In these cases, the Cloud user should negotiate to enter a term that allows him to read the terms of the subcontracting entity and give him the right to terminate the contract in case he disagrees with the sub-contracting. The Cloud user should also include a term in the Service Level Agreement that if the Cloud Provider fails to meet his requirements as described in the contract the user has the choice to terminate the contract. Sometimes, there is term that the Service Level Agreement is subject to the Cloud Providers Policies. The user should ask to read these policies in order to determine whether they are acceptable by him and clarify whether he is bound in cases that these policies change at a later point of time. The Cloud Standards Customer Council has issued a "Practical Guide to Cloud Service Level Agreements" that provides the steps that consumers should take to evaluate cloud Service Level Agreements in order to compare cloud service Providers or negotiate terms with a provider [5].

An additional concern is related to the development of a number of Cloud Computing projects that usually use automated mechanisms for compliance with terms of the Service Level Agreement. The CloudScale project which assists service Providers in analyzing, predicting and resolving scalability issues [6] has guidelines (CloudScale's HowTos) to solve the scalability issues detected and can define the service consumer 's services according to the agreed SLA as well as the Responsibilities of Service Provider to fulfill SLA. In Cloud-TM project a SLA model has been proposed in which when the offer has been accepted by the customer, there is a method to ensure that network equipment's are configured to guarantee the contracted SLA parameters [7]. There are a variety of projects that include as part or final step solutions for the monitoring mostly of the agreed SLAs. Assuming that all requirements of the traditional contract law has been met in order to have a valid contract (e.g. consent, meeting of the minds, acceptance, consideration) there might be an issue of what happens if the parties (Cloud user and Cloud Provider)comply with these methodologies but an error occurs. Who has the responsibility of the system error?

III. WHO CAN SUE THE CLOUDPROVIDER?

The "Privity of contract" principle means that a contract is concluded only between its parties and with no other person as well as the contract can be enforced only by the parties of the contract and by no other person. The "Privity rule" applies to the contract concluded between the Cloud user and the Cloud Provider. Thus, only one of these parties cans sue the other. Although, the doctrine of privity of contract means only that the party of the contract can bring an action on the contract, nevertheless this party is not excluded from the possibility that he may have some other additional causes of action e.g. on tort.

Although, the most common contract is between the Cloud user and the Cloud provider, other contracts may also exist. For example, the Cloud Provider may enter into a contract with a platform Provider in order to use its platform or contract between the Cloud Provider and an infrastructure Provider for the provision of the infrastructure for the services. The contract principles apply to all these situations. And only the parties to these contract can sue each other.

The liability regime of Cloud Providers and consequently who is eligible to claim damages from them are related to the core business of Cloud Providers. The extent of liability of Cloud Provider's is related with only the person or entities that are possibly entitled to claim compensation for damages either due to breach of contract or due to other obligations imposed by other laws. Moreover, as a consequence of the duty of care, the Cloud Provider is liable to whom it owns this duty. Thus, Cloud Providers might also have potential liability under tort law either to its users or any third party who has injured from its behavior like third parties whom their Intellectual property rights have been infringed by the use of the Cloud provider's software. In all cases the determining factor is the wording of the signed contract since it is this fact that is going to determine the magnitude of loss.

IV. JURISDICTIONAL ISSUES

The advert of Cloud Computing created a marketplace that requires a global approach towards a coherent and predictable framework. One of the important elements of Cloud Computing is that data are moving and it is questionable which court can adjudicate a case of potential dispute or which law applies-particularly when data are moving through different jurisdictions. However, there is a need for certainty and predictability for the Cloud Computing contracts since both individuals and businesses want to know the requirements they need to comply with. Compliance is not possible without knowing which laws are applicable to the Cloud contracts as well which law applies to a potential dispute

Therefore, the essential question is how to find the proper Court that has the authority to adjudicate the potential dispute as well as which law regulates Cloud Computing contracts. Jurisdictional principles have been traditionally developed for contracts concluded in the same sovereignty emphasizing to the presence and domicile of the defendants within a particular sovereignty.

Thus, territoriality provides a fundamental determinant for the assertion of personal jurisdiction. Nevertheless, considering the dynamic allocation of Cloud Computing tasks it is questionable whether the traditional jurisdiction principles apply and to what extend can regulate cross border Cloud Computing contracts.

If parties have chosen jurisdiction for the adjudication of their Cloud contract this is valid clause on the contract. Nevertheless, this is questionable when the Cloud Provider contract is presented as standard form contract-click wrap agreement. The forum selection clause might be invalidated on the basis of the inequality of bargain among the parties. In this case, as well as when there is not such clause in negotiated contracts, there are a variety of issues that need to be considered in order to determine the proper applicable law.

Moreover, the issue of personal jurisdiction for Cloud Computing contractual disputes over nonresident defendants is a confusing one. Initially, for the assertion of jurisdiction, the determinant factor was the defendant's present while latter the consent factor was also added. Still these bases for personal jurisdiction has proven to be inefficient, thus the Courts applied the minimum contacts test which examines the relationship between defendant and the forum. This test comes with uncertainties especially when there is only one contract with the forum that needs to satisfy the minimum contacts test. The Courts in order to address the increasingly complicated situations added to the minimum contacts test the reasonableness test. This test requires additionally that the minimum contacts of the defendant with the forum should be of such nature that does not offend traditional notions of fair play and substantial justice

Courts examine additionally, besides the requirements of minimum contacts and reasonableness, whether the defendant has purposely avail himself to the forum, whether his activities are targeted intentionally to the forum as well as whether he has created continuous obligations with the particular forum. If the calculation of these parameters results to the conclusion that the defendant conduct is such that it looks reasonable to anticipate for him to be hauled in the specific forum, then there is basis for personal jurisdiction. In the process of this calculation other factors are considered additionally such as the interest of the forum State to adjudicate the case, the public policies of the forum, and the degree of burden that the decision will create to the defendant.

How these principles apply to Cloud Computing is highly questionable. The unique characteristic of Cloud Computing is the transfer of data through multiple jurisdictions. Each country at the same time has different law applicable to jurisdictional issues. Usually if parties have not decided upon applicable law, then the law of the closest connection with the contract will apply. The proper law in this case should be inferred from the terms, circumstances and all related matters to the contract. This is known as the "inferred test". The thing is how to determine these factors and apply to Cloud Computing contracts. What constitutes minimum contact at Cloud? It looks that there is no uniform rule for the finding of proper law in Cloud Computing contracts. These principles could be applied in analogy to this environment and decided on a case by case basis. In each case the Court should examine the route of the data through the various nodes and the significance of the processing of these nodes in order to determine the applicable node. Further analysis is beyond the scope of this work.

V. CONTRACTING OUT CLOUD USER'S DATA PROTECTION RIGHTS

The Cloud management system provides a platform where users can access data from anywhere in the world [8]. Data and data processing are protected by data protection laws thus exposing the Cloud Provider and the Cloud participants to liability issues. Moreover, the regulation of data protection rights is regulated differently in various jurisdictions. When data are given to the Cloud Provider through the client or an intermediary, the Provider partitions and replicates data in the Cloud infrastructure. Can the client claim that the data is not used for the purpose collected? How can the Provider guarantee that each participating node will use the data only for the specified purposes? Another issue is whether the user (the Cloud client) is entitled to access his/her data held by the Cloud Provider and if it is appropriate to correct or erase such data. Additionally, while the user might have the right to request and obtain access to his/her data from the Cloud Provider, it is not clear whether this access includes revealing information regarding where the data reside and other information regarding the Cloud nodes that store and process the data. Moreover, the data circulation in Cloud Computing is dynamic. The transfer of data is decided based on the availability of nodes that can execute the task at the specific point in time and the replication optimizing the performance of the Cloud at the specific point in time. These are real time decisions that cannot be pre-defined. Also the rules that govern such decisions are part of the logic of the software of the Cloud Provider and many times not publicly available.

In the healthcare sector cloud solutions are becoming more and more appealing, since they can offer significant cost reductions. Health care monitoring systems are systems that are responsible for tracking the health of the patient. The patient himself can insert data collected from heath devices or the devices can be connected to the system and submit data. In each case several data are collected from a variety of patients in different formats. For example collected data could be X- rays, temperature, hear bits, blood pressure etc. When coupled with telemedicine applications [9], the patient monitoring system can provide an integrated remote healthcare service for patient diagnosis and treatment. Cloud computing environment is considered as an approach that allows real-time data accessibility with authentication and real time video streaming to support the teleconference. Moreover, cloud enables the exchange of information between Healthcare providers in an efficient manner.

One of the issues that the Healthcare provider needs to consider when deploying applications in the cloud is that existing solutions do not address the security requirements demanded by the sensitive health care data. Detailed analysis of these issues is beyond the scope of this work. However, a well drafted contract between the Cloud Provider and Cloud user or the contract between the Cloud Provider and the platform or infrastructure Provider could ensure efficient and balanced protection. The contract should facilitate the lawful and fairly circulation of data within the Cloud environment and specify the obligations of the Cloud provider. In a Cloud Computing contract users usually do not object to have the Provider collect and publish cumulative statistics provided that the data cannot be manipulated to obtain information about a specific record or a specific data source.

In cases where data mining algorithms are allowed to execute in the data they should guarantee that the algorithm produces statistics that guarantee privacy.

Furthermore, it seems that a visible solution could be that appropriate software should be provided (by the Cloud Provider to the user) to allow the user to view and update the application data as well as his/her personal data. The software should be able to inform the user regarding the number of nodes that execute his/her application, the number of partitions made of the application data and the number of replicas of the data at the moment of request. Moreover, there is a question whether the Cloud Provider can by contract with the Cloud user waive the users' privacy and data protection rights. If the Cloud user consents to waive his data protection rights does this constitute a valid contract based on the principle of freedom of parties? Does contract law preempt the data protection law? The answer to this question is not straightforward. It has to be addressed in the specific context of the contract and in relation to the specific legislation.

VI. GOVERNMENT OF INDIA AND CLOUD COMPUTING

India government has implemented an initiative called GI Cloud or Meghraj. The focus of this initiative is to evolve a Strategy and implement various components including governance mechanism to ensure proliferation of Cloud in Government[10]. The Government of India has implemented a number of Information and Communications Technologies (ICT) initiatives under the National e-Governance Plan (NeGP), including creation of ICT infrastructure both at the centre and state levels[4,11]. The infrastructure thus created will provide the basis for adoption of cloud computing for the government with the objective of making optimum use of existing infrastructure, thus helping achieve the ultimate goal of NeGP[11].

A task force has been set up to give necessary direction with respect to the various activities which include creation of a detailed plan on the cloud strategy, cloud architecture, cloud implementation plan and roadmap[12]. DeitY set up two committees : the GI-cloud Task Force under the chairmanship of Additional Secretary (e Governance) to propose policy and guidelines for "Government as a user of Cloud Computing" and the Cloud Computing Working Group to work out the recommendations for evolving a comprehensive framework by the Government for adoption of Cloud in the country taking into account the policies and standards relating to jurisdiction, cross-border data flow, data security, data location etc. and other related aspects for enabling cloud services in India[13].

The Jammu & Kashmir state government adopts cloud computing for its e- Governance services. The Government, using the State Data Centers based out of Madhya Pradesh, is provisioning e Governance services such as issuing death or birth certificates and trade licenses through the cloud. The Jammu & Kashmir Government uses Microsoft's solution to implement cloud computing.[14]. The state of Jammu & Kashmir is the first state that utilized cloud computing services[15].

CDAC has established a Private cloud environment to offer basic cloud services such as Infrastructure, Platform, and Software service to Government and SMEs[9]. CDAC has numerous projects at Cloud such as Meghdooth which is free and open source. Cloud stack developed by CDAC Chennai is a one stop solution for implementing in Cloud environment. One of the remarkable activities ongoing is Integration of Private Cloud computing environment with existing Garuda Grid (India's National Grid Computing Initiative)[16].

Moreover, the National Telecom Policy 2012 has recognized that the advent of technologies like cloud computing present a historic opportunity to enhance India's service delivery capabilities to a new level domestically as well globally, enable social networking and m-Commerce at scale which were not possible through traditional technology solutions[17]. The Confederation of Indian Industry, in a report titled "The Indian Cloud Revolution" has stated that there is a need for statutory compliance to laws and regulations. The report concludes that a set of necessary rules and regulation should be created by the Government such as those related to privacy and confidentiality to protect against accidental access to information [18].Cloud computing helps also in good governance since it makes easy the transfer of data and reduce the cost of ICT infrastructure. The adoption of cloud computing enhances the effectives of e-Panchayat as well as it will bring better result in governance especially in rural India[19]. The benefits of adopting cloud services in agriculture sector which contributes 20% to India's GPD and is the biggest employment source it will be a serious attempt to develop rural India. Gujarat Government realized the importance of cloud computing services and has identified the importance of electronic contracts on cloud. There are several contractual constraints to be addressed by the contractual agreements between clients and providers that are not adequately addressed by the cloud computing interface such as the data location and security[20]. An interesting initiative is that of the University of Pune (UoP) that announced it will use cloud computing for its exam systems in four faculties [21]. Part of literature argues that Cloud Computing applications should be employed by Indian Railway because it will allow for the exact calculations of numerous situations that currently cause loss to the Indian Railway [22].

Additionally, the Department of Electronics and Information technology has a FOSS Initiative cell to develop and support Free/ Open Source Software in India[23] with a Free and open source Division[24]. NRCFOSS has come out with BOSS – Bharat Operating system Solutions with support for Indian Languages. Indian Government adopts OS applications e.g. among others, the Government of Tamil Nadu has issued a governmental Order that makes mandatory the installation of BOSS in all computer systems and should be used by Staff Members of Information Technology Department, the Government has launched the IT@ School project in Kerala, the Open government Platform in cooperation with the U.S. Government[25].

Moreover, the Unique Identification Authority of India (UIDAI) [26]has introduced the Aadhaar[27]project which uses open source for software development[28] The principal engineer for Aadhaar, Regunath Balasubramanian, explained [29] that open source became the first choice because technical requirements required vendor neutrality and FOSS helped achieved vendor neutrality which is very important for a initiative for national importance. However Aadhaar is not totally based on open source components and during its implementation to states that completely under open source created problems like interoperability problems. Kerala has found that Aadhaar is problematic and unacceptable since its implementation violates the States FOSS policies[30].

The issue thus, that need to be addressed is how the India Government would be able to combine cloud computing and open source solutions in accordance with its regulatory framework. The open source licenses are not compatible with cloud computing contracts. Thus, a specific legal framework need to be developed to solve these issues.

VII. CONCLUSION

Cloud computing has shifted the internet transactions from a centralized to a distributed environment which enable users to use data and software located in the internet rather their computers or their servers. The employment of Cloud Computing is associated with substantial benefits for its participants such as cost reductions, new business models, new services offered as well as new ways of reaching markets. This phenomenon comes with a set of opportunities as well as major challenges. One of these challenges is its regulation since the legal framework for operating in Cloud computing will be critical in determining the pace of the development of the Cloud.

The analysis of the Cloud computing related contracts affirms that the Cloud Computing establishment and its increased use create concerns due to uncertainties of its legal framework. These uncertainties refer mainly, but not exclusively, to the validity of contracts with the Cloud Provider (including Service Level Agreements) and more specifically with the limitation of liability clauses presented in these contracts. The contracts with the Cloud Providers often include confusing terms regarding who is liable particularly in cases of errors that cause damages. Generally, the enforceability of standard Service Level Agreements are viewed as analogous to click wrap contracts. That view creates a presumption that these contracts are valid as long as the assent of the Cloud user has been affirmed. However, it is unclear whether the Cloud user has given a valid acceptance. The employment of traditional contract principles functions as a patchwork since it cannot address the peculiarities and novel issues raised by the use of Cloud computing. Thus, the current legal framework cannot regulate adequately the Cloud computing environment and therefore a new legislation need to be enacted which will exclusively regulate the legal framework of Cloud computing applications.

A proposed solution might be the enactment of a specific legislation on Cloud Computing by the Indian Government - that legislation will be the first of its kind- establishing a coherent and secure legal framework which will prescribe in a sophisticated and effective manner the Cloud Computing legal environment for both Governmental and Industrial applications

REFERENCES

[1]The Restatement (Second) of Contracts(USA), § 1, Contract Defined

[2]The Indian Contract Act 1872, section 2(h)

[3]W. Kuan Hon, Christopher Millard and Ian Walden., "Negotiating Cloud Contracts: looking at clouds from both sides down", 16 Stan. Tech. L. Rev. (2012), p.81

[4]Lee Badger et al., US Government CloudComputing Technology Roadmap, Volume I, Release 1.o (Draft), High Priority requirements to Further USG Agency CloudComputing Adoption, 2011, http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeI-2.pdf

[5]Cloud Standards Customer Council, "Practical Guide to Cloud Service Level Agreement", version 1.0, http://www.cloudstandardscustomercouncil.org/2012_Practical_Guide_t o_Cloud_SLAs.pdf

[6]www.cloudscale-project.eu

[7]https://www.ict-etics.eu/fileadmin/documents/news/ETICS_white_paper_final.pdf

[8]A. Khan, P. Shaikh, C. Dhembre and S. Gawali, " Cloud Services for Collaborative Web Based Project Management System", 8 International Journal of Computer Science Issues (2011), p.180

[9]P. Matlani, N.D. Londhe, "A cloud computing based telemedicine service," Point-of-Care Healthcare Technologies (PHT), 2013 IEEE , pp.326-330, 16-18 Jan.

[10] Government of India Ministry of Communications and Information Technology, Department of Information Technology, Free and Open Source Software, http://deity.gov.in/content/free-and-open-source-software

[11]Government of India Ministry of Communications and Information Technology, Department of Information Technology, Free and Open Source Software, http://deity.gov.in/content/free-and-open-source-software

[12]Government of India, Ministry of Communications & IT ,Department of electronics and Information Technology "GI Cloud (Meghraj)Adoption and Implementation Roadmap", April 2013

[13]NASSCOM, "Government of India Cloud initiative", http://www.nasscom.in/government-india-cloud-initiative

[14]Arun Chandrasejaran and Mayank Kapoor, Frost & Sullivan 2011-Market Insight, " State of Cloud Computing in the Public Sector- A Strategic analysis of the business case and overview of the initiatives across Asia pacific

[15]The Economic times, "J&K uses MP govt's cloud computing facilities to roloout egovernance", http://articles.economictimes.indiatimes.com/2010-06-25/news/27582997_1_data-centres-cloud-model-cloud-services

[16]Cloud Computing at CDAC, http://www.cdac.in/index.aspx?id=cloud_ci_cloud_computing

[17]Government of India, Ministry of Communications & IT ,Department of electronics and Information Technology, "Government of India's GI Cloud (Meghraj)Strategic Direction Paper", April 2013, http://deity.gov.in/sites/upload_files/dit/files/GI-Cloud%20Strategic%20Direction%20Report(1).pdf

[18]Confederation of Indian Industry, " The Indian Cloud Revolution", http://www.cii.in/cloudreport

[19]Chasura R.S. et al., "Cloud Computing : future Buzz for Rural India", Wayamba Journal of Animal Science, (2012), p. 255

[20] An e-governance bulleting from Gujarat Informatics LTD., "Cloud Computing", 7 GIL, 2010

[21] Ardhra Nair, " UoP to introduce cloud computing in four faculties", The Indian Express, 2013, http://www.indianexpress.com/news/uop-to-introduce-cloud-computing-in-four-faculties/1100723

[22]Gaurav Bhatia et.al., " Implementation of cloud Computing Technology in Indian Railway", 37 IPCSIT (2012), p.84, International Conference on Information and Network Technology (ICINT 2012)

[23] Government of India Ministry of Communications and Information Technology, Department of Information Technology, Free and Open Source Software, http://deity.gov.in/content/free-and-open-source-software

[24]Government of India Ministry of Communications and Information Technology, Department of Information Technology, Free and Open Source Software, http://deity.gov.in/content/free-and-open-source-software

[25] Open Government Platform, http://www.opengovplatform.org/

[26]Identification Authority of India, Planning Commission, Government of India, http://uidai.gov.in/

[27] Unique Identification Authority of India, Planning Commission, Government of India, Aadhaar, http://uidai.gov.in/aadhaar.html

[28] PK Jayadevan, " UID: Due to the technology challenges of speed and scale, Aadhaar is an objectof attention", The Economic Times, 2012, http://articles.economictimes.indiatimes.com/2012-02-07/news/31034068_1_aadhaar-project-unique-identification-authority-biometric-database

[29] Vandana Sharma, "Aadhaar: A Testimony to Success of FOSS in India", Linux for you 2011, http://www.linuxforu.com/2011/12/aadhaar-testimony-to-foss-success-in-india/]that

[30] Deepa Kupur, "Aadhaar software locked in with "Windows", The Hindu, 2010, http://www.thehindu.com/news/national/aadhaar-software-locked-in-with-windows/article863657.ece