ISSN: 2582-6433

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed6th Edition

VOLUME 2 ISSUE 7

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

Cloud Computing: From A Technolegal Lens

Authored By-Sonika Lakra & Jitesh Kadian

Cloud Computing : The Concept

Cloud computing involves a subscription based service that satisfies computing and storage needs from a virtually unlimited hardware and communication infrastructure which is managed by a third-party provider. Put it a bit differently, cloud computing occurs when an internet connection delivers hardware power and software functionality to users regardless of where they are or which computer they are using. NIST (National Institution of Standards and Technology) defines it as "Cloud is a model for enabling convenient, on demand network access to a shared pool of all configurable computing resources (storage, networks, services, servers and applications) that are easily released and rapidly provisioned with minimum management effort." Needless to say, the five critical characteristics that form the hallmark of the above standard definition are – on demand self service, broad network access, rapid elasticity, resource pooling and measured services. By contrast, the Gartner Group defines cloud computing as a style of computing in which massively scalable IT – related capabilities are provided as a service using internet technologies to multiple external users.

Clouds are essentially data centres or server farms on which software and data can be remotely stored, instead of on- site. It is a natural evolution of distributed computing and the general variation of virtualization and service oriented architecture (SOA). Cloud computing activities are often described as falling into one or more of the following service categories:

Infrastructure as a Service (IaaS): raw computing resources such as processing power and storage.
Platform as a Service (PaaS): platforms for developing and deploying software applications (Google App Engine is a classic example)
Software as a Service (SaaS): end user applications
Apart from the above three service models, there are four deployment models too – public, private, hybrid and community. The essential characteristics of all these models are

(I) Pay as per use

(II) Use it as and when required

(III) Services provided by a third party service provider

(IV) No change in the ownership of the main property.

ISSN: 2582-6433

Rationale Behind Cloud Computing

The genesis of cloud computing days back to the early 2000s when organizations started spending money to set up their IT infrastructure for improvement of business by purchasing own dedicated server. As the day progressed, these servers became virtual and easily available publicly through internet. Thus the cloud was born as a model that is easily manageable, accountable and configurable. Perhaps the best example of this kind of service is one that is almost ubiquitous now : web-based email services like gmail and hotmail. From legal research to word processing, file storage and movie viewing, computer users are able to take advantage of the cloud for a variety of tasks –some mundane and some others extremely sensitive and highly technical (storing and securing personal information for millions of credit card subscribers or health records for insureds being classical examples). Google has introduced Google Chrome OS, an operating system designed to function almost completely through the cloud providing essentially remote computing software that can be updated automatically through the web.

No discussion on cloud computing will be complete without the case study of Animoto – a software provider that converts personal photos into music videos it developed a Facebook application that took the company from 25000 users to 2,50,000 users in three days . At its peak, Animoto was signing up 20000 new users per hour. It launched the service with five virtual servers and by the end of three days expanded to 3500 servers. Animoto's ability to scale up at such an incredible rate was accomplished by using a cloud provider that was able to add resources as demand for product increased. Mention also needs to be made of the increasing popular concept of netbooks – low cost light weight laptop computers with reduced hardware capacity and processing power – that provide users with vast resources because the cloud is fully accessible. Today companies such as Google, Facebook and Microsoft who need to process large quantities of data operate numerous massive cloud data centres that may each occupy tens of thousands of square feet and contain thousands of computers. Like Feynman's Los Alamos team – narrated in his wonderful auto biography "Surely You're Joking, Mr Feynman" – these computing complexes provide computing as a service for many people.

What Cloud Computing Can Offer Us : The Next Generation Of Internet

The existing internet provides us content in the form of videos, emails and information served up in webpages. With cloud computing, the next generation of internet will allow us to "buy" IT services from a web portal, drastically expanding the types of merchandise available beyond those on e-commerce sites such as eBay. We would be able to rent from a virtual store front the basic necessities to build a virtual

ISSN: 2582-6433

data center – such as CPU, memory and on top of that the middleware necessary : web application servers, databases, enterprise server bus etc as the platforms to support the applications we would like to either rent from an independent software vendor or develop ourselves. Together this is what we call “IT as a Service” (ITaaS) bundled to us – the end users – as a virtual data center.

Advantages of Cloud Computing

Cloud computing offers the following advantages :

Scalability in terms of resources : A company can start small and increase its hardware resources as it needs.
Flexibility in terms of the different software packages and operating systems
Pay – as – you – go economic model borrowed from utility computing
Consolidation of System Maintenance and Management : this overhead is shifted from cloud users to its providers
Reliability : The system’s fault tolerance is managed by the cloud providers and users no longer need to worry about it
High utilization and reduced carbon footprint as typically a large number of custom servers is consolidated into a smaller number of shared servers.
Legal Issues

Cloud computing service providers – whether global or regional – will inevitably run up against international law, particularly data protection law and privacy regulations. Each country has its own set of laws – some being dramatically more stringent than others . There are no laws unique to the cloud. But the cloud brings with it some legal issues which while not applying only to the cloud are perhaps now uniquely important to those operating or using a cloud-based service. The most important among these pertains to sovereignty on the internet: location and use of data.

A key question with any cloud computing service is “where is the data stored or processed?”. The reality in this regard is that even the cloud service provider may not know where the data is residing.

Unlike a fixed server in the office or at a data centre, data in the cloud could potentially be located anywhere in the world – even in multiple data centres in multiple copies worldwide. Read these with the fact that cloud computing services involve processing of masses of data that is often commercially sensitive, confidential and “personal information” and the picture is complete. To put it a bit differently, sending and processing data around the globe could in the process fail to comply with data protection and privacy laws in various countries. The EU for example provides a strict legal regime under the EU Data

ISSN: 2582-6433

Protection Directive where unless certain steps are taken, companies can be prohibited from transferring personal information to countries that do not give the same level of protection. If a European company is processing data on the cloud and is processing personal information in the EU, it may not be complying with EU laws if data is moved to countries outside the EU.

The Classic Case Of Microsoft Corporation Vs US District Court

No discussion on the legal issues pertaining to cloud computing can be complete without a reference to the Microsoft Corporation case. Microsoft is a major player in the cloud industry with a 12% market share. Their innovation – Office 365- is a highly popular cloud based office software and email platform.

It all started in 2013 when the Justice Department asked for access to the email account contents and Microsoft refused that query with a response that data which are not stored in US is outside of US jurisdiction. In 2014, the US District Court for the Southern District of New York issued a search warrant (under the SCA 18 USC) seeking access to the contents therein whose data was stored in Ireland. Francis M.J, the US judge issued the warrant since he believed that the government presented enough evidence to support the belief that the mail account was being used for narcotics trafficking. Microsoft delivered all contents of the mail account whose data were stored in locations inside US, but advised that the most valuable data were located in their Irish

based storage and that to provide the same they would need to transfer the data from Irish based storage to US based storage which they declined to do. Instead they requested for revocation of the warrant. But the District Court denied the motion to quash and ruled Microsoft to be in civil contempt.

Microsoft‘s contention was that a warrant intrinsically includes territorial restrictions and hence in the present case does not cover Europe. The government on the other hand argued that the warrant was applied as a compelled disclosure similar to a subpoena. Therefore the actual physical location of the object is of no consequence if it is under the control of Microsoft and can be delivered by them.

Upon having their motion to quash the warrant dismissed, Microsoft appealed to the US Court of Appeals. The Court deduced that the warrant is against extra territoriality as it may bring international conflicts. Since Microsoft satisfied the warrant by providing all data that were stored in US and only refused to provide data stored outside US territory, the Court of Appeal lacked authority to enforce the warrant. Thus the US Court of Appeals (2015) reversed the District Court’s dismissal of the request to quash the warrant.

The aforesaid case has had profound implications on the future of internet privacy, ethics in technology, respecting other countries borders and user’s privacy. It needs special mention here that Microsoft successfully illustrated that no matter how big or small the case is, the company take privacy of users very

ISSN: 2582-6433

seriously. However the persistent nature of US government's attempts to access user's data without their consent has sent shivers down many spines. In a kneejerk response, many users have signed cloud service contracts with oversees cloud providers. Another situation is for users to encrypt their data. Mention must be made here of the Open Whisper Systems encryption algorithm which is known for its high reliability. In fact, the algorithm is so reliable that governments would not bother to request access to the users' data as they know that even if the data is supplied, encryption will mean that it is not possible to view the contents. Add to these the fact that many countries have decided to pass "data localization laws" and the picture is complete.

The US case is not the first one wherein Microsoft was requested to provide users' data nor will it be the last time. For instance, in 2013, Brazil asked Microsoft for the same kind of access, but it was for access to Skype application data located outside of Brazil. Microsoft refused to provide the data. The result was that the Brazilian authorities arrested the local manager of Microsoft in January 2014.

The EU, it needs to be mention here, takes this kind of transaction very seriously. An example is a case wherein the European authorities found that by virtue of a US court's order, the Belgium based branch of an international bank and the SWIFT (Society for Worldwide Interbank Financial Telecommunications) provided some financial transaction data of a European citizen to the US government. Belgium found this act to be a violation of EU privacy law. SWIFT was forced to change its network structure in order to remove any possible future transfer of European data to outside of EU unless it complied with EU data privacy legislation.

Issues Pertaining To Lock In

A major concern of cloud computing is lock in which refers to the complexity to switch from one cloud service provider to another. Needless to say, it increases dependency on the service provider. Questions that arise in this context are:-

Is the data portable between service providers ?
If service providers change, can the records be accessed ?
What are the obligations on each party regarding an exit plan?
Vint Cerf, the computer scientist who is often called the father of the internet, has identified the issue of moving data between clouds as one of vital importance. According to him, developing intercloud standards and protocols so that data does not get caught in one cloud is the equivalent now of the issues faced in 1973 when networks could not communicate with each other.

ISSN: 2582-6433

Concerns Of Data Security

Unlike the traditional model wherein users had control over their data and could implement whatever safeguards they thought necessary to retain control, cloud users neither possess nor control their data. This raises serious apprehensions on the data security front. The issue vis-a-vis cloud computing is that the customer using the services is not aware what part of their data is getting saved on their device and what is getting saved on the cloud. In fact, data security in the context of cloud computing has to be analyzed in the backdrop of the triad concepts of confidentiality, integrity and availability.

Confidentiality is the anticipation of intended or unintended unauthorized disclosure of contents whereas integrity guards both data and system against any illegal modification or deletion thereby ensuring originality and nonrepudiation of data. Availability on the other hand gives the assurance of trustworthy and timely access of information. This concern centres on critical applications and data being available. Well publicized incidents of cloud outages include gmail's one-day outage in mid October 2008, Amazon S3's over seven – hour downtime on July 20, 2008 and Flexi Scale's 18 hour outage on October 31, 2008. Availability also means the extent to which user's data can be recovered when accidents such as hard disk damage, fire and network failures occur. Viewed from this triad, the security issues in cloud computing can be categorized into three broad classes – traditional security concerns, availability issues and third party data control related issues. Common security concerns in the cloud are:-

Data breaches :- The chances of data breaches or losses increase in cloud environment. According to a research carried out by the Ponemon Institute titled "Man in Cloud Attack", the likelihood of over all data breaches is three fold in a cloud environment.
Hijacking of Accounts:- Hackers having login information to remotely contact data in cloud can cause hijacking. Moreover they can manipulate data through captured credentials.
Denial of Service Attack:- it tries to make websites and servers unavailable to legitimate users.
Insider Threat:- Employees can utilize authorized access to misuse or access sensitive information.
Abuse of Cloud Service :- It affects both the service provider and its client
Insecure APIs (Application Programming Interfaces)
Malware Injection:- These are scripts/codes embedded deliberately into cloud service. Once executed, attackers can eaves drop and compromise integrity.
Side Channel Attacks:-An emerging concern for cloud delivery models using virtualization platforms is the risk of side channel attacks causing data leakage across co-resident virtual machine instances.
Transfer to public cloud involves a change of responsibility and giving accessibility of data to the provider. This can be ensured by building clauses in the contract with the provider which have appropriate provisions for security and help in maintaining legal protections for data stored.

ISSN: 2582-6433

The user also must ensure foolproof services within their own systems. Issues like standard of the services being provided, the ownership of IP, service level agreements, liability regimes, warranties and indemnity provisions, confidentiality obligations and termination clauses must all find their places in the contract for cloud based services. Needless to say, the various requirements imposed by law will subsist in addition to the terms of the contract. A classic example in this regard is the provision regarding liability of the parties under the Australian Trade Practices Act.

An interesting example of the inadequacy of standard terms and conditions to meet the expectations of a business user can be seen from a successful bid by Google to provide cloud based services to the city of Los Angels[i]. The contract included unlimited damages for data breach, guarantees as to where the data will remain and penalties if the services are not available for longer than five minutes a month.

No discussion on data security in the context of cloud computing will be complete without a reference to mash-up authorization. As adoption of cloud computing grows, more services performing mash-ups of data will be witnessed. A case study in this regard is provided by Facebook, the users of which upload both sensitive and non-sensitive data. This data is used by Facebook to present data to other users and this data is also utilized by third party applications. Since these applications are typically not verified by Facebook, malicious apps running in Facebook's cloud can potentially steal sensitive data.

Problems Vis-A-Vis Data Privacy

Privacy refers to the right of self determination. It is the ability of an individual or group to seclude information about themselves and thereby reveal them selectively. It has the elements of when, how and extent. A good reference for use in defining universal principles for the protection of personal data and privacy is the Madrid Resolution (2009). The basic principles that must govern the use of personal data include those of lawfulness and fairness, proportionality, purpose specification, data quality, openness and accountability. It needs to be mentioned here that there is a huge divide between developed and developing countries in terms of adequate legislation of protection of personal data.

In the cloud, privacy means when users visit sensitive data, the cloud services can prevent potential adversaries from inferring the user's behaviour by the user's visit model. ORAM (Oblivious RAM) is a promising technology in protecting privacy in the cloud.

No discussion on confidential and sensitive data in the context of cloud computing can be complete without a mention of the Odense Municipality case. The view of the Municipality was that sensitive data about students and parents can be processed in Google Apps. However, the Municipality's use of cloud computing to store sensitive information was rejected by the Danish Data Protection Agency (DDPA).

ISSN: 2582-6433

The case confirms that a serious risk assessment must be made before switching to cloud services. It also points out that standards should play an essential role in fostering adoption thereof.

Issues Pertaining To Incomplete Data Deletion

A major concern of cloud computing is that it is always possible that data has not been properly deleted and that multiple copies or traces may have been stored. When users delete their data with confirmation, all copies of data should be deleted at the same time. Cloud storage providers should ensure that the deleted data of users cannot be recovered and used by other unauthenticated users. This is particularly important in the backdrop of data recovery technologies that could recover data deleted by users from the hard disks. To avoid data be recovered and unauthenticatedly used, a possible approach is to encrypt the data before uploading to the cloud storage space. A classic example is FADE system which is based on technologies such as Ephemenzer.

Cloud Service Providers And Liability For Content

Cloud providers are by no means exempted from any accountability if the material that users store in the service is the ground for a civil or criminal offence. The general rule in this regard is that the provider is exempt from liability for illegal or infringing content on its servers if the following two conditions apply:-

It has no part in determining the content of the transmission or it has no knowledge or control of illegal information stored on its servers and
It acts expeditiously to remove or prevent further storage and transmission of any illegal information it is made aware of.

The latter requirement is referred to as notice and take down obligation.However due to the differences in the various regimes, the applicability thereof to cloud computing services must be evaluated on a case-by-case basis, depending on the provisions of the specific country and nature of the service provided on the cloud. In particular, cloud providers in EU and US can generally benefit from all the liability exemptions generically offered to ISPs (Internet Service Providers).

Concerns Regarding IPRs

These concerns are closely connected to the question: Who owns the data in the cloud? The answer lies in the observation that normal copyright rules apply if the data being stored in the cloud is fit for copyright

ISSN: 2582-6433

protection (ie) it has some degree of novelty and is the product of author's intellectual work. Thus the user of the cloud service can very well have the author's right over the work. However, the cloud terms of service may include provisions according to which the provider has some power over the data stored in the cloud. This is not an actual copyright transfer, but the author might be limited in exercising his monopolistic rights over the copyrighted material. Ownership of IP can be eroded by a formal agreement or dedication of the work to the public domain, but in the cloud computing environment, mere uploading of information in a cloud platform does not entail losing IPRs. But it is important that the rights over the content in the cloud be kept well distinct from rights over cloud assets. By doing so, it is possible for the cloud customer to avoid undesired consequences such as loss of IPRs to the cloud provider. Conversely, the provider's IPs need to be protected horizontally from unfair business practices by competitors and vertically from possible illicit behaviours by customers. Thus the provider will hold exclusive ownership over the rights used in providing the cloud service (ie) it owns IPRs to the software and the customer will be granted a license to use the technology. In the PaaS and IaaS delivery models, separation of ownership for applications developed by the customers and the tools used to develop them should be made clear in the contract terms. Mention also needs to be made here of the Japanese initiative towards introduction of a new form of IP protection for big data.

Concerns Regarding Bandwidth Costs

With cloud computing, companies can save money on hardware and software, but they could incur higher network bandwidth charges. Bandwidth cost may be low for smaller internet based applications, which are not data intensive, but could significantly grow for data-intensive applications.

Laws, Standards And Regulations Pertaining To Cloud Computing

These Fall Into Four Broad Categories:-

Compelled disclosure to the government
Classic examples are

USA : Stored Communications Act (SCA), Electronic Communications Privacy Act (ECPA), National Patriot Act and Fair Information Practice.
UK : The Regulation of Investigatory Powers Act
Australia : Privacy Act in the APPs, APP12:Access to Personal Information, Freedom of Information Act 1982

ISSN: 2582-6433

Moreover policies of national cryptography in UK, Singapore, Malaysia etc may allow a court order to access cryptography.

Regulations dictating how a cloud service provider protects customer data security
Examples are

USA : Gramm – Leach – Biley Act (GLBA), Health Information Technology for Economic and Clinical Health (HITECH), Family Educational Rights and Privacy Act (FERPA)
UK : Privacy and Electronic Communications (EC Directive), Data Protection Act and Directive
Australia : Privacy Act in the APPs, APP 11: Security of Personal Information
Relating to transfer, retention and privacy of data between the clients and the data storage provider

Examples are

USA : FTC Fair Information Practice, Payment Card Industry Data Security Standard (PCIDSS), Freedom of Information Act
UK : The Safe Harbor Agreement (defined in data transfer between USA and Europe)
Australia : Privacy Act in the APPs, APP 8 : Cross-border disclosure of personal information, Privacy Act 1988 – Section 16C, Privacy business resource & Sending personal information overseas
Relating to physical location of data storage servers
Examples are

USA : Payment Card Industry Data Security Standard (PCIDSS), NARA regulations
UK : Euro Data Protection Directive
Australia : Privacy Act in the APPs, APP 8 : Cross-border disclosure of personal information
The Legal Framework For Cloud Computing In India

Cloud computing services that deal with personal or sensitive information need to comply with the requirements set out under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 relating to security, encryption, access to data subject, disclosure, international transfer and publication of policy statements. Thus a cloud computing service company before trading with “sensitive personal information” having a link to India has to make sure to be in observance with the aforesaid Rules as any non-compliance would invite penalties and imprisonment. Cloud service providers in India may also be required to comply with the Information Technology (Intermediaries Guidelines) Rules 2011.

ISSN: 2582-6433

In addition to the IT Act and Rules, use of cloud computing in banking and insurance sectors is subject to specific restrictions. The RBI's guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks sets out specific requirements to be complied with by banks while engaging cloud service providers. These requirements inter alia relate to vendor selection, data security, form of agreement, business continuity and disaster recovery or management practices. On the other hand, the Insurance Regulatory and Development Authority of India's Guidelines on Information and Cyber Security require insurers to comply with requirements in relation to data, application and network security, indent management and information security audit while using services from a cloud service provider.

Conclusion

Cloud services are the best method to offer a dynamic and self adjustable computing and storage resource service to a wide range of clients – from residential users through small businesses to large multi-national organizations. A cloud is a pool of virtualized computer resources and can host a variety of different workloads, including batch-style backend jobs and interactive, nay user-facing applications. It supports redundant, self- recovering, highly scalable programming models that allow workloads to recover from many unavoidable hardware/software failures. However a word of caution is needed here – the cloud ecosystem must be designed to be secure, trustworthy and dependable. Cloud security faces different challenges and issues at various levels in the form of vulnerabilities and attacks – multitenancy, cloud secure federation, vendor lock in , loss of control, confidentiality, data integrity and privacy, data intrusion, virtualization vulnerabilities, cloning and resource pooling, UM hopping, XML signature attack, XSS attack, SQL injection attack and flooding attack, to name a few. Moreover, international law is not agile enough to compete with cloud computing developments. The onus therefore is on international cloud service providers to be familiar with data protection laws and policies of each country that they have a presence in – regardless of their essential understanding about the technology that they are providing via their platforms. In addition, the policies regarding data transfer between countries need to be seriously accounted for in their business plans.

Issues surrounding development of standards and best practices in the areas of interoperability, escrow and privacy need to be addressed along with questions as to whether adequate due diligence has been carried out along the chain of responsibility. Otherwise cloud service providers will be exposed to an avalanche of claims including those pertaining to liability for data mining and liability under securities laws for improper dissemination of investment information on social networking websites. The currently pending cases including class action litigations pertaining to Netflix Inc, Facebook "Beacon" Google "Buzz" should be eye openers in this regard. Mention also needs to be made here of the emergence of a parallel

ISSN: 2582-6433

form of business called cloud brokering whose objective is to guide the potential enterprise in the choice of a cloud service provider, untwining the tangle of differential features. In a de jure condendo perspective, a uniform legislative approach would be advisable. Internet services operate in a global market. Hence a unified approach – possibly one based on a WIPO treaty – would provide benefits to cloud customers by establishing uniform terms and conditions which drive consistency in the protection of data in the cloud. Opinions are galore that a "cyber seas" agreement may be the ideal vehicle for this kind of system because it provides a balance between a state's ability to regulate the cloud and an over seeing international authority. Taking the prudent steps now to harness the cloud may in the near future allow the world to reflect on an entirely man-made global public utility and the beginnings of a truly cooperative world market. Needless to say, ultimately it is the users who will choose the model that makes the most sense given their needs – which may end up being a hybrid of cloud computing and the traditional model.

References

Al – Khouri AM, Data ownership : who owns my data? Int J Manag Inf Technol 2007, 2(1); 1-8

Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A et al, A view of cloud computing, Commun ACM 2010; 53(4);50-58

Azeez A, Perera S, Gamage D, Linton R, Siriwardana P, Leelaratne D et al, Multi-Tenant SOA Middleware for Cloud Computing in Proceedings of the 3rd International Conference on Cloud Computing (CLOUD)2010; 458-465, IEEE

Bartolini C L, El Kateb D, Le Traon Y, Hagen D, Cloud Providers Viability: how to address it from an IT and legal perspective ? in Altman J, Silaghi G C, Rana O F Editors Economics of Grids, Clouds, Systems and Services Vol 9512 Computer Communication Networks and Telecommunications, Springer International Publishing, 2016; 281-295

William Voorsluy, James Broberg and Rajkumar Buyya, Introduction to Cloud Computing in Cloud Computing: Principles and Paradigms (Wiley 2011)

Mark H. Wittow and Daniel J Buller, Cloud Computing: Emerging Legal Issues for access to data, anywhere, anytime in Journal of Internet Law, Aspen publishers 14(1),2010