International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 4 • 2017

Cloud Computing with special reference to Data Security

Rashmi K. Aggarwal[1], Rajinder Kaur[2], Teena Bagga[3] and Namita Bhardwaj[4]

[1] *Professor, Institute of Management of Technology, Ghaziabad*
[2] *Professor, University Institute of Legal Studies, Panjab University, Chandigarh.*
[3] *Associate Professor, Amity Business School, Amity University Uttar Pradesh*
[4] *Research Scholar, Department of Laws, Panjab University*

Abstract: Corporate sector's requirements of computing and data storage are managed by IT industries. The Cloud computing technology has marked a paradigm shift in the IT sector by making the facilities of computing and data storage in the form of utility service, just like electricity. The users can use computing services without making huge investments in developing and managing IT infrastructure, but simply hiring it as utility service which the user can use according to its requirements. Given the fact that India is a developing country, cloud computing is a green solution to the heavy infrastructure investments made by the companies where they can hire compute facilities and store data on the data centres of third party cloud service providers. Despite of the low cost and higher efficiency offered by cloud computing, the biggest threat it poses to the users is Data protection and security. The present paper discusses the issue of data security and protection and i[1]s divided into five parts. The first part is the introduction which explains the meaning and concept of cloud computing, its service and deployment models, advantages and disadvantages. The second part discusses cloud computing in corporate sector and deals with the issue of data protection in cloud computing. The third part discusses the legal provisions regarding Cloud computing in India. The fourth part contains the judgements regarding Liability of Intermediaries. The fifthS part talks about the Data Protection laws in other countries. The last part of the paper concludes the same.

1. INTRODUCTION

Cloud computing refers to enabling provisions of computing, data storage, applications, and services through internet by Cloud service providers. This internet based computing technology has brought a paradigm shift in the IT sector as computing and data storage facilities are now available as a service, thereby removing the need for investing in huge infrastructure for computing and storage operations. The users can process and store their data in the data centres of cloud service providers. It is based on a 'pay as you go' model and allows multiple users to use same shared computer processing resources. The economies of scale which cloud computing offers, makes it the most appropriate model for corporate firms to adopt. The pace, with which the cloud services are gaining importance in the corporate sector, is unmatched with the potent legal threats it poses. Of the various unaddressed legal issues, the most important is Data Protection and Security. Although India does not have any specific legislation on Data Protection,

the Information Technology Act, 2000 contains provisions regarding data protection and security. The paper attempts to discuss the various legal issues emerging out of data protection and security in cloud computing and the remedies available for Data breach in context of India.

Cloud computing is defined by to National Institute of Standards and Technology (NIST) of the U.S. Department of commerce as "Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1] The five essential characteristics as listed by NIST are [1]:

a. On- demand service- A customer can unilaterally stipulate computing capacities, such as server time and network storage, as needed mechanically without requiring individual dealings with each service provider.
b. Broad network access- capacities are accessible over the set of connections and accessed through standard means like mobile phones, tablets, laptops and workstations.
c. Resource pooling- The provider's computing funds are shared to provide several customers via a multi-tenant form, with diverse material and virtual assets vigorously allocate and relocate according to customer claim.
d. Rapid elasticity- capacities can be elastically stipulated and released, in some cases mechanically, to scale swiftly external and internal proportionate with claim. To the customer, the capacities available for provisioning often appear to be unrestricted and can be appropriated in any quantity at any time.
e. Measured service- Cloud systems without human intervention manage and optimise resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and consumer of the utilised service.[1]

Cloud computing can be accessed via following facility model. First is 'Infrastructure as a service (Iaas)' under which, hardware facilities like data centres, virtual computers, network infrastructure are made available as a service. Amazon web services, Microsoft azure are the examples of the same. This model is on the whole used by huge corporates who prefer renting computing services than investing in huge IT infrastructures. Second model is 'Platform as a service (PAAS)' under which, computing platforms like web servers, database operating systems and programming environments are used for initial claim without the need of installing the tools on computer systems. This model is preferred by software developers. Example: Google apps engine. Third model is 'Software as a service (SAAS)' under which, software applications are made available to the end users by cloud service providers. Google docs, sales force are the examples of the same.

Cloud services can be installed through any of the subsequent four models. In a 'Public cloud', cloud services are available to the general public and can be shared by different users. Public cloud provides elasticity and cost- effective means to manage computing needs. In a 'Private cloud', cloud services are deployed exclusively for a particular organisation. It can be managed on premise or off-premise the organisation. It offers more data security and protection than a cloud, but is costlier to run than a public cloud. In a 'Hybrid cloud' it is a mix of public and private cloud, where the user can combine the services of both the clouds. In a 'Community cloud', the cloud services are shared amongst several organisations engaged in similar activities.

One of the biggest advantages of cloud computing is cost effectiveness. As the users don't have to invest in infrastructure, it brings down the cost of computing. Cloud computing services can be

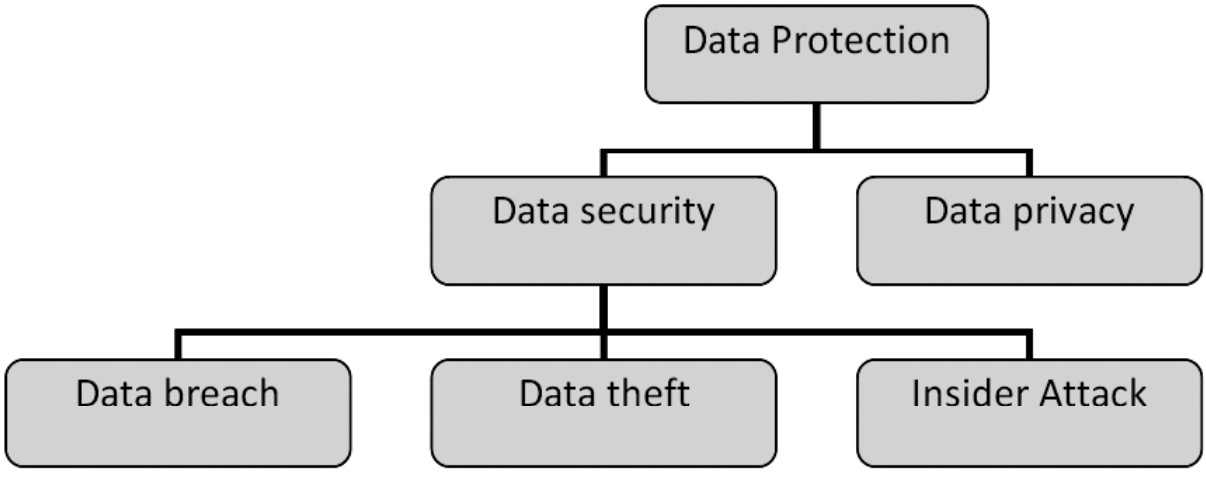
easily scalable up or down according to the needs of the user. It offers flexibility, as it is based on a 'pay as you use' model, where the users pay according to the services used, thereby eliminating the need to own and manage infrastructure or software applications. It increases efficiency and saves resources.

Despite the benefits of cloud computing, there are many risks attached to it. Firstly, as the data is stored in the data centres of cloud providers, the responsibility of data protection and security shifts to the cloud service provider. Secondly, the sensitive and personal data on cloud is at risk of phishing attacks, identity thefts, etc. Thirdly, as cloud is based on a multi- tenant model, there are possible risks of loosing data integrity as the cloud is shared by multiple users. Fourthly, there is risk of compromise on data privacy as the data is handled and managed by a third party.

2. CLOUD COMPUTING IN CORPORATE SECTOR

Cloud espousal in India is on a mounting binge which will outshine the whole world. According to research firm Gartner, "As telecommunication technology entrée, e- business, cellular phone device and apps usage and trade agreement keep on to increasing, the growth in cloud related spending in India should surpass that in the rest of the world and possible reach $1.9 billion by 2019"[2]. India's ambitious project 'Digital India' focussed on enhanced communications and superior internet availability is also an attractive factor for cloud suppliers like IBM, Microsoft, and Amazon is expanding their cloud procedures in India. As the report by Department of Commerce of United States i.e. *ITA Cloud Computing Top Markets report*[3] states that India is ranked at number eight as a prospective marketplace for cloud services. It is also supported by 2015 Asia Cloud Computing Association report named *SMEs in Asia Pacific: The Market for Cloud Computing* – The main attraction for cloud adoption in India by corporate sector is Reduced Costs [4].

With the initiation of internet and now the Cloud Computing technology, various legal disputes have occurred concerning data protection. The possible rise in cloud services also increases the probable hazard of data contravention or data loss which scythes has stern consequences on the trade, goodwill and reputation of the company. Cloud data hacks like "Operation high roller" in 2012 which drain off $ 2.5 billion from bank accounts in Europe, U.S.A., Columbia[5]; and the latest scything of "Dropbox"[6] in August, 2016 cloud in which the passwords of 68 million individuals have been hacked demonstrates the menace cloud computing regarding the sensitive and individual data. The twin dangers i.e. security and privacy are relating to data protection. The following are the major challenges in data protection in a cloud environment.



2.1. Data Security

a. Data Infringement- As cloud is based on multiple tenancies or multiple leasing model the cloud service supplier may be careless in controlling the data of the users, consequential in data loss or identity.

b. Data Stealing/ theft- In a cloud service, as the data of the consumer is stock up in the data- hub of cloud service supplier; the consumer is not in charge above the data and is more exposed to theft by other consumer on the cloud.

c. Insider attack- A lot of corporate scams have been a consequence of data leak by the employee of the company which can cause massive damage to the customer. Where the businesses are leaking the sensitive facts can result into grave consequences on the processes of the business.

2.2. Privacy and confidentiality

Privacy and Confidentiality both are the significant facet of data protection. As most of the individual facts vis-à-vis health, finance, inclinations of a human being is accessible on the internet nowadays, its protection is very necessary. Invasion into the peculiar particulars of an individual lacking his consent would amount to breach of privacy.

3. LEGAL PROVISIONS IN INDIA ON DATA PROTECTION

With the advent of internet and cloud computing technologies, various legal challenges regarding protection of data and information have arisen. Although India does not have a dedicated legislation on data protection, but it is enclosed under Information Technology Act, 2000 which provides for the protection and preservation of data.

Cloud Service Suppliers are covered under the definition of *'Intermediaries'* under Section 2(1)(w) of the Information Technology Act, 2000, which covers a) individuals who on behalf of another person receives, stores or transmits any electronic record, or b) provides service with respect to that record. The key purpose of cloud computing is to deliver computing technology in the form of service; hence cloud service suppliers are well covered within this definition.

The law in India regarding the liability of intermediary favours the intermediary, and not the end user. Section 79 of the Information Technology Act, 2000 provides that intermediaries are not responsible for any third party data, information or communication link made available by them; subject to various conditions which are as follows:-

a. The first condition is that the role of Cloud Service Provider as an intermediary should be limited only to *providing access to a communication system*, over which information made available by third part is transmitted or temporarily stored or hosted.

b. Secondly, the Cloud Service Supplier *does not have any control over the transmission.* Thus, the Cloud Service Provider should not:

    a. Start the transmission,

    b. Select the receiver of the transmission, and

    c. Select or modify the information contained in the transmission.

c. Thirdly, the Cloud Service Supplier must notice *due diligence,* while discharging his duties. The obligations of due diligence are mentioned under the Information Technology (Intermediary Guidelines) Rules, 2011.

d. Fourthly, the Cloud Service supplier has *not conspired or abetted or aided or induced*, whether by threats or promise or otherwise, in the commission of any unlawful act.

e. Fifthly, the Cloud Service Supplier, *upon receiving actual knowledge* or being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource, controlled by the Cloud Service Providers, is being used to commit the unlawful act, the provider, expeditiously removes or disables access to that material on that resource without vitiating the evidence in any manner whatsoever.

Rule 3 of Information Technology (Intermediaries Guidelines) Rules, 2011 explains the obligations of 'Due diligence' which provides for the publication of rules and regulations privacy policy and agreement for access or usage of the intermediary computer resource not to host, notify, display, upload, modify, publish, transmit, update or share any information which is not users, resulting to violation of trademark, copyright or other intellectual property rights, infringes the law which is applicable, misleads about the source of information, imitate another person, comprises viruses and dangers the security, sovereignty, unity, integrity of India.

Thus, where a person binds crime under Information Technology Act, 2000 on a cloud setup or by using a cloud service provided through a cloud service supplier, then prima facie liability would be of that person. The liability of cloud service provider as an intermediary would arise only if he has conspired or abetted or aided or induced the commission of any unlawful act; or if he has not complied with the due diligence rules; or if he on receiving actual knowledge or being notified by the appropriate Government of unlawful act on its cloud, does not remove it.

Situations of Data Protection breach and the remedies under Information Technology Act, 2000:-

a. Failure to protect personal or sensitive data- Section 43A of the Information Technology Act, 2000 provides for the civil remedy for failure in protecting data by the company possessing and dealing with such data. Whereas, Section 72A deals with criminal liability for failure to protect data.

Section 43A sets out that a body corporate will be liable to pay Damages by way of compensation to an affected person, when:

- Such a *body corporate,* possesses, deals or handles
- Any *sensitive personal data or information* in a computer resource which it owns, controls or operates, and
- Is *negligent* in implementing and maintaining *reasonable security practices and procedures,*
- Causing *wrongful gain or wrongful loss* to any person.

The provision is supplemented with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or information) Rules, 2000.

Rule 3 of the above- mentioned Rules defines Sensitive personal data or information as information relating to password; financial information such as Bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information; any detail relating to the above clauses as provided to body corporate for providing service; and any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise[7].

Rule 8 of the above-mentioned Rules explains the compliance of 'Reasonable security practices and procedures'. It states that a body corporate shall be considered to have complied with reasonable security

and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. The rule provides the International Standard IS/ISO/ IEC 27001 on "Information Technology- Security Techniques- Information Security Management System Requirements" as one of the standards which have to be adopted.

Section 72A of the Information Technology Act, 2000 explains the criminal liability in case of failure to protect data. It states that when any person including an intermediary who while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the *intent* to cause or *knowing* that he is likely to cause wrongful loss or wrongful gain discloses without the consent of the concerned person or in breach of a lawful contract, such material to any other person shall be an offence. The punishment for the said offence shall be imprisonment for a term which may extend to two years, or fine which may extend to five lakh rupees or both.

Thus, in a situation of cloud hack, data theft, data loss on involving sensitive and personal data information, companies can invoke this section 43A or Section 72A of the Information Technology Act, 2000.

b. Data privacy- Section 72 of the Information Technology Act, 2000 provides for penalty for breach of privacy and confidentiality. It states that:- If any person, in pursuance of any of the powers under the Act, has secures access to any electronic record, book, register, correspondence, information, document or other material, then he is duty bound not to disclose the same to any other person. If he discloses any of the above-mentioned details without the person's consent, he will be punished for an imprisonment which may extend to two years, or fine which may extend to one lakh rupees, or with both. Under the Information Technology Act, 2000, the persons on whom power is vested to access the electronic records of another include:- the Controller of Certifying Authorities, Deputy Controller, Assistant Controller or any other officer authorised by them, Certifying Authorities and adjudicating officers.

The present section has a very limited scope and is restricted to violation of privacy by the above-mentioned statutory authorities, who have secured access to the data in pursuance of the statutory powers conferred to them.

c. Offences by companies- Instances of insider attacks have become very common, especially in cases of data leak of sensitive and personal data of a company by its own employees. It generally involves leaking of personal information of customers of that company. Eg- leaking of credit card details. In such cases, Section 85 of the Information Technology Act, 2000 fixes the responsibility of companies. Section 85 states the procedure followed where companies commit any offence under Information Technology Act, 2000. The section states:- Where a company commits a contravention of any provisions of the Information Technology Act, 2000 or any Rules, directions or orders made thereunder, the company as well as every person, who at the time of contravention was in-charge of the company, shall be responsible and guilty of the contravention[8]. However, such a person shall not be liable if the person liable for punishment proves that the contravention took place *without his knowledge* or that he exercised all *due diligence* to prevent such contravention. Where the contravention of any provisions of the Act has been done with the consent of any director, manager, secretary or other officer, then such a person will be liable under this section.

d. Preservation and retention of information by intermediaries- Intermediaries are huge depositories of information. This may include information relating to illegal or criminal acts. Such information

\might be required by the Government for investigation purposes. Section 67C deals with preservation and retention of the relevant electronic information and logs by intermediaries. Section 67C of the Information Technology Act, 2000 provides for prevention and retention of information by intermediaries for duration and manner prescribed by the Central Government. Any intermediary who intentionally or knowingly contravenes Section 67C, shall be punished with imprisonment which may extend to three years and also be liable to fine.

4. JUDGEMENTS REGARDING LIABILITY OF INTERMEDIARIES

The first landmark judgement on liability of intermediaries was in the case of *Avinash Bajaj v.State* where CEO of Bazee.com was arrested in connection with display of pornographic material on its website. The facts of this case is that a student of IIT Kharagpur posted a post of two school children engaged in an explicitly sexual act on the online auction website Bazee.com. the CEO of the company was arrested as it was held that the company in its capacity as an intermediary failed to exercise due diligence as it allowed to display content that was pornographic in nature. After this judgement, there was a huge uproar by the Indian corporate sector regarding the applicability and interpretation of Section 79 of the Information Technology Act, 2000. In 2008, the section was amended which diluted the liability of intermediary to a large extent. Recently, in the case of *Shreya Singhal v. Union of India*, which declared Section 66A of the Information Technology Act, 2000 constitutionally invalid, also discussed the constitutional validity of Section 79 also. Holding the section as constitutionally valid, it also upheld the Information Technology (Intermediaries Guidelines) Rules, 2011, with a slight change that intermediary will remove any electronic content only on order of competent court or relevant government agency.

5. DATA PROTECTION LAWS IN OTHER COUNTRIES

The EU Data Protection Directive 95/46/EC has been so far the most important directive issued in the context of data protection. It lays down that personal shall not be processed unless certain conditions of transparency, legitimacy, purpose and proportionality are compiled [9]. In *United Kingdom,* there is a dedicated legislation on data protection, The Data Protection Act, 1998 which lays down principles to be followed before processing data. In *U.S.A.*, there are various acts dedicated to data protection. The Gramm-Leach- Bliley Act, 1999; Electronic Communications Privacy Act,1986; The computer Fraud and Abuse Act,1986; The Health Insurance Portability and Accountability Act,1996; Fair Credit Reporting Act and Fair and accurate credit transaction Act, 2003; Children's information: Children's online privacy protection Act; Privacy Act, 1974 are numerous acts which provide for data protection of online data or information, financial transactions, medical history and children information[10].

6. CONCLUSION

Gains of Cloud Computing technology will be unfruitful if the risks and dangers associated with it overshadow the benefits it offers. From the point of view of corporate firms opting for cloud adoption, the liability of the cloud service provider as an intermediary, in the case of failure to protect data on the cloud arises only if he has not complied with due diligence requirements as provided under the Information Technology (Intermediaries Guidelines) Rules, 2011 or if it is done intentionally. *Shreya Singhal* judgement has further delayed the remedy of an affected person who is affected by offensive content put on the computer network or resource of an intermediary, where he cannot directly approach the intermediary for removing the content but has only two options of either going to the court and getting an order of removing the offending content or approaching a governmental agency for notifying the intermediary to remove the content. The issue of privacy is very narrowly restricted under the Act to making liable only statutory authorities having authority over electronic data, misusing their power by disclosing the data without the

consent of the person whose data is being compromised. The Information Technology Act, 2000 fails to address the most common problem of breach of data privacy. Although the Information Technology Act, 2000 has established compliances of reasonable security practices and procedures for protecting electronic data and information, a well defined dedicated legislation on Data protection is the only answer to encourage the corporate sentiment for adopting cloud services for running cost effective and efficient businesses.

REFERENCES

[1] Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing*, Special Publication (NIST SP) – 800-145 (September 28, 2011). Available at http://dx.doi.org/10.6028/NIST.SP.800-145 (accessed on 1st September, 2016)

[2] Sony Shetty, *Gartner says Indian Public Cloud Services Market Will reach $731 million in 2015*, Gartner Newsroom, October 26,2015. Available at http://www.gartner.com/newsroom/id/3156617 (accessed on 2nd September, 2016).

[3] 2016 ITA Cloud Computing Top Markets report . Available at http://trade.gov/topmarkets/pdf/Cloud_Computing_India.pdf (accessed on 2nd September, 2016)

[4] Asia Cloud Computing Association, SMEs in Asia Pacific: The Market for Cloud Computing. Available at: http://www.asiacloudcomputing.org/images/ACCA_SMEReport2015_Final.pdf

[5] Michael B. Kelley, *Operation High Roller: This Massive Cyberattack has siphoned as much as $2.5 billion from World banks*, Business Insider. June 28, 2012. Available at http://www.businessinsider.com/operation-high-roller-2012-6?IR=T. (accessed on 1st September, 2016)

[6] AFP, *Dropbox hacked, 68 million passwords leaked on the internet,* The Economic Times. September 2, 2016. Available at http://economictimes.indiatimes.com/magazines/panache/dropbox-hacked-68-million-passwords-leaked-on-the-internet/articleshow/53972955.cms. accessed on 2nd September, 2016

[7] Pavan Duggal, Law of intermediaries 112 (Universal Law Publishing, 1st edition 2016)

[8] Pavan Duggal, Law of intermediaries 112 (Universal Law Publishing, 1st edition 2016)

[9] Pavan Duggal, Law of intermediaries 112 (Universal Law Publishing, 1st edition 2016)

[10] Rosemary P Jay, *Data protection and privacy*, 2015. 208 (Law Business Research Ltd, 2015). Available at https://www.huntonprivacyblog.com/files/2011/04/DDP2015_United_States.pdf. accessed on 9th May, 2016.