International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Regulatory Compliance for Cloud Computing in India: An Overview

Shakti Kumar

Assistant Professor S.K.J Law College

ABSTRACT:

Cloud Computing emerged as a transformative technology which enables data storage and service delivery over the internet. It also provides scalable and flexible solutions to meet the demands of businesses, government entities, and individuals.

In India, cloud computing is still in its early phase of development and initiatives like Digital India and the National e-Governance Plan taken by the central Govt. aiding in its growth. The Indian legal system has not fully adapted to meet the specific requirements of cloud technology. The present statute, the Information Technology (IT) Act of 2000, only addresses electronic records, digital signatures, and cybercrime, but fails to cover the unique legal and regulatory challenges of cloud computing, cross-border data transfers, data privacy, and service provider liability.

This paper will explain the various legal, security, and compliance issues associated with cloud computing in India and will also highlight the lack of a dedicated regulatory framework and international data regulations, such as the European Union's General Data Protection Regulation (GDPR), which influence global cloud practices, raising concerns about compliance for Indian companies engaged in cross-border operations.

The paper also examines the IT Act's limitations, emphasizing the need for updated laws and standards to address issues specific to cloud services, including data localization, user privacy, data portability, and accountability of cloud providers. It suggests that adopting best practices for data security, enhancing regulatory guidelines, and establishing a robust legal framework could enable India to leverage cloud computing more effectively while safeguarding users' interests.

Keywords: Cloud computing, Data Security, Data Privacy, Jurisdictional Issues, Information Technology Act of 2000,

1. INTRODUCTION:

Cloud computing is a technique of storing data and information through hosted services over the internet, primarily used by IT service companies to deliver storage needs to end recipients. It relies heavily on resource and data sharing, allowing organizations to quickly start and manage their applications. However, the large concentration of information at a single centre makes it more susceptible to cyber-attacks, and the excessive power given to cloud companies to manage resources increases the risk of untrustworthy conduct. The system is currently in its emerging stages in India, but its effectiveness is questionable due to cloud providers' lack of due diligence.

Cloud computing refers to an infrastructure that offers on-demand resources or services over the Internet, depending on the scale and reliability of a data centre. It includes storage, data, and compute clouds, which

are stacked together to serve as a computing platform for developing cloudbased applications. Examples include Google's GFS, Amazon's S3 storage cloud, Simple DB data cloud, EC2 compute cloud, and the open-source Hadoop system. High-performance computing systems assume that processors are scarce resources and shared, with data moved to processors when available. This is known as the supercomputing model, which simplifies the process, while the data centre model involves storing data and co-locating computation with it when possible. Cloud computing platforms like GFS/MapReduce/BigTable and Hadoop have been designed with two main limitations. Firstly, they assume all nodes are co-located within one data centre or have a small bandwidth between geographically distributed clusters. Secondly, they assume small individual inputs and outputs to the cloud, despite large aggregate data. This is because most clouds target Web applications that collect and process large numbers of small Web pages. However, some e-science applications require large datasets and processing, and queries for certain applications may result in large datasets being returned.

2. Meaning of Cloud Computing:

The term cloud is a metaphor for the internet itself. The term **"cloud computing"** wasn't coined by a single person, but its development can be attributed to several key figures and companies over time. The concept of cloud computing dates back to the 1960s, with early ideas attributed to pioneers like John McCarthy, who predicted that "computation may someday be organized as a public utility" in a speech in 1961. However, the term “Cloud Computing” in its modern sense, focusing on remote data storage and processing services provided over the internet, began to take shape in the early 2000s.

Formally in 2006, this term was popularized and defined by Eric Schmidt, then CEO of Google, who described it as a new model for delivering computing resources online. However, the National Institute of Standards and Technology (NIST) gave the most widely recognised and referenced definition in 2011. NIST defined cloud computing as:

"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 National Institute of Standards and Technology (NIST) also identifies five essential characteristics of cloud computing[2]: -

1. **On-demand self-service**: Consumers can provision computing resources automatically, without requiring human intervention from the service provider.
2. **Broad network access**: Cloud services are available over the network and can be accessed through standard mechanisms that promote usage by heterogeneous thin or thick client platforms.
3. **Resource pooling**: Cloud providers pool resources to serve multiple consumers, with resources dynamically assigned and reassigned based on demand.
4. **Rapid elasticity**: Capabilities can be elastically provisioned and released to scale quickly according to demand.
5. **Measured service**: Cloud computing resources are metered and billed based on usage, allowing for a pay-as-you-go model.

[1] NIST. (2011). *The NIST Definition of Cloud Computing* (Special Publication 800-145). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-145

[2] NIST. (2011). *The NIST Definition of Cloud Computing* (Special Publication 800-145). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-145

In 2011, Mell and Grance, in their NIST report, defined cloud computing as a model for delivering computing resources (e.g., processing power, storage, and services) on demand through a shared pool of resources. This model allows users to access these resources over the internet with minimal management effort. The report stresses that cloud computing enables businesses and individuals to focus on their core activities without the need to maintain IT infrastructure. Additionally, it emphasizes the flexibility, scalability, and cost-effectiveness of cloud computing, where users can scale resources based on their needs and pay only for what they use.[3]

In 2012, the European Commission outlined cloud computing as the delivery of computing services, including storage, processing power, software, and applications, over the Internet rather than from local computing infrastructure. It emphasizes that cloud computing services enable the provisioning of computing resources on-demand and with pay-per-use pricing, which can improve scalability, efficiency, and flexibility for businesses and individuals. The Commission focuses on the economic potential of cloud services, stressing the ability to reduce costs, improve productivity, and enable innovative business models across various sectors.[4]

Cloud Computing allows consumers and businesses to use applications without installation and access their files stored online. Earlier, various software applications had to be installed on a single system. With the advent of cloud computing, a single application provides the user with access to a web-based cloud that hosts all the programs necessary to accomplish word processing as well as all the other computing needs of a person. A cloud user will never have to face the loss of data because the hard drive of his PC has crashed or software has been corrupted. If a Cloud subscriber's PC fails or is stolen, the subscriber only has to download his data from the cloud and will not even have to restore the files from the backup or otherwise try to restore his data from his PC.

In short, Cloud computing refers to the technology that provides software, data access, and storage devices that do not require the physical location of the system. The main advantage over the conventional forms of application is that cloud computing need not depend upon the physical structure of its operation. A very interesting feature of cloud computing is interoperability of various interfaces is imperative. Accordingly, the development of cloud computing will necessarily promote the growth and use of open-source software.[5]

4. Types of Clouds

There are four primary cloud computing deployment models as outlined by the National Institute of Standards and Technology (NIST). Each model is designed to meet different organizational needs related to control, security, and flexibility in the use of cloud resources.

1. Private Cloud (Internal Cloud)
2. Hybrid Cloud
3. Public Cloud
4. Community Cloud

[3] Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing* (Special Publication 800-145). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-145

[4] European Commission. (2012). Cloud Computing: Benefits, Risks and Security Issues. European Commission, Directorate-General for Information Society and Media.

[5] Laurin H. Mills, "Legal Issues Associated with Cloud Computing," Nixon Peabody, May 13, 2009.

Private Cloud (Internal Cloud):- It is a cloud infrastructure that is exclusively dedicated to a particular company or organization. [6] It offers the organization complete control over its resources, security measures, and data management. This model is ideal for companies or institutions that deal with highly sensitive or proprietary information, as it allows them to implement strict security protocols and compliance measures. Private clouds can be hosted either on-premises (within the organization's own data centres) or externally by a third-party service provider, but the cloud infrastructure remains dedicated to one organization. This means that even if the cloud is hosted by an external provider, it is not shared with other organizations. Private clouds are often used by large enterprises or government agencies that require stringent control over their data and applications.

Public Cloud: It is a cloud computing model where services are provided to the general public over the Internet.[7] A public cloud is owned by the provider selling cloud services and is external to the user's organisation.[8] These services are typically offered by third-party cloud service providers, such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud, and are accessible to anyone who has an internet connection. Public clouds are the most commonly used for Software as a Service (SaaS), where applications like email, file storage, and collaborative tools are hosted and accessed over the web. Public clouds are ideal for smaller businesses, startups, and individual users who do not need to maintain control over infrastructure or manage high-security requirements. They are often chosen because they are cost-effective and easily scalable, offering a "pay-as-you-go" pricing model that makes them financially attractive for smaller-scale operations.

Hybrid Cloud: A hybrid cloud is a combination of both private and public clouds, offering the best of both worlds that remain separate cloud entities, but share certain technology that permits interoperability.[9] It allows organizations to store and manage sensitive or critical data and applications on private cloud infrastructure while utilizing public cloud resources for less sensitive workloads. This flexibility enables organizations to meet their security, compliance, and operational needs while benefiting from the scalability and cost-efficiency of public cloud services. For example, an organization might use a private cloud for confidential financial data but run web applications or customer relationship management (CRM) systems in the public cloud. Hybrid clouds are often used by large enterprises that need to maintain a certain level of privacy and security but also want to take advantage of the flexibility of public clouds for specific tasks.

Community Cloud: A community cloud is a cloud infrastructure shared by several organizations that have similar concerns or needs, such as compliance, security, or jurisdictional regulations, rather than maintaining their separate cloud infrastructures, these organizations

share resources to meet common objectives.[10] Community clouds are often used by industries such as government, healthcare, education, and finance, where regulatory compliance (such as HIPAA in

[6] Wayne Janse and Timothy Grance, U.S Department of Commerce, NIST, "Guidelines on Security and Privacy in Public Cloud Computing," Special Publication 800-144., January 2011, p.3.
[7] Wayne Janse and Timothy Grance, U.S Department of Commerce, NIST, "Guidelines on Security and Privacy in Public Cloud Computing," Special Publication 800-144., January 2011, p.3.
[8] Wayne Janse and Timothy Grance, U.S Department of Commerce, NIST, "Guidelines on Security and Privacy in Public Cloud Computing," Special Publication 800-144., January 2011, p.3.
[9] Wayne Janse and Timothy Grance, U.S Department of Commerce, NIST, "Guidelines on Security and Privacy in Public Cloud Computing," Special Publication 800-144., January 2011, p.3.
[10] National Institute of Standards and Technology (NIST). (2011). *The NIST Definition of Cloud Computing* (NIST

healthcare or GDPR in Europe) is crucial. For example, multiple government agencies might use a shared community cloud that provides secure infrastructure tailored to their specific legal and security requirements. Community clouds offer the benefits of shared resources while ensuring that participating organizations can meet their unique requirements.

5. Legal Issues regarding Cloud Computing: -

Cloud computing introduces various complex legal issues arising from its unique architecture, cross-border data movement, storing and processing of huge amounts of data in the cloud and dependence on external service providers. Here are some of the primary legal issues:

A. Privacy issues: what can the cloud provider do with the user data

Cloud providers often manage huge amounts of personal data from millions of users of cloud service, and the data from one user commingles with the data of other users.[11] There was a debate on cloud computing and privacy from a settlement in Author's Guild, Inc. v. Google Inc.[12] The stipulations of the agreement permitted Google to keep on offering copies of books on their cloud-based Google Books platform in return for a stipulated amount to the authors. Although privacy was not the main concern in the settlement, many public interest organizations were alarmed that the agreement did not acknowledge the security of the privacy of its users.

The issue raised by Consumer Watchdog in 2010 was that the settlement "still contained no restrictions on what data could be gathered, and contained only limited restrictions on how that data cloud be shared". The settlement agreement did not address whether a user's reading preferences could be shared with news outlets or governmental units acting without a search warrant. Consumer Watchdog was concerned that the settlement gave Google a monopoly over the book search and book subscription markets and at the same time gave it unrestrained authority to share private information about users with outside entities.

A group of objecting class members to the Google settlement, Privacy Authors and Publishers, asserted that the lack of privacy protection in the Google settlement agreement would deter readers from reading and purchasing their works.[13] According to the Privacy Authors, if readers were worried that information about their reading habits could be disseminated to the government, divorcing spouses, or other interested third parties, these readers would be less likely to view books on controversial topics. Not surprisingly, the Privacy Authors included several authors who had penned books on sensitive or controversial subjects.

B. Jurisdiction confusion: which laws apply to the data in the cloud?

The amorphous collection of servers, applications, and data that makes up "the cloud" lends itself to potential jurisdiction conflicts. The jurisdictional question is an important one because of the display in privacy laws; if a company does not know which jurisdiction its data is subject to, how can it know which laws apply? In the United States, for example, the Patriot Act gives the government broad latitude to intercept suspicious electronic data that comes through the country.[14] "European and Asian companies have expressed concerns about having their data stored on computers in the U.S.A. which fall under the

Special Publication 800-145). https://doi.org/10.6028/NIST.SP.800-145

[11] William Jeremy Robison, Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act, 2010 GEO. L.J. 1195.

[12] Author's Guild, Inc. v. Google Inc., No. 058136(DC), 2009 WL 5576331(S.D.N.Y. Nov. 13,2009)

[13] Author's Guild, Inc. v. Google Inc., No. 058136(DC), 2009 WL 5576331(S.D.N.Y. Nov. 13,2009)

[14] H. R. Cong. Res. 3162 107th Cong. (2001) (enacted)

jurisdiction of the USA Patriot Act, allowing the U.S. government to access that data very easily."[15] On the other hand, in the European Union, the data protection directive puts stringent standards on the collection of electronic data by the government and by any other entity.[16] Because of these distinctions, it is important that cloud computing or SaaS (Software as a service) agreements specify where the data is physically located and which laws apply. Yet another statutory hurdle to cloud computing in the United States is the Health Insurance Portability and Accountability Act ("HIPAA").[17] HIPAA places substantial restrictions on the transfer and disclosure of private health information. For example, entities that are covered by the Act must enter a business associate agreement with cloud providers before the providers can store records containing health information in the cloud.[17] Because of HIPAA's requirements, it is important for foreign entities to know where their data is located.[18] This knowledge ensures that they can enter the necessary agreements with the cloud provider to avoid liability under HIPAA.[19]

Cloud computing agreements do not just cause jurisdiction confusion internationally. Privacy Laws also vary from state to state within the United States. For example, a law in Massachusetts requires anyone who holds personal information belonging to a Massachusetts resident to implement a detailed written security program to protect the data.[20] Companies subject to these regulations that want to implement cloud computing must determine whether the cloud provider maintains adequate security measures to protect its electronic data. Because a Massachusetts resident's data could be commingled with the data of many other users in the cloud, it would be difficult for cloud providers to know which state regulations applied to such providers. With the business world rapidly embracing cloud computing solutions, it is only a matter of time before litigation arises that directly addresses the jurisdictional problems with cloud computing.[21]

C. Contributory liability for infringement

In addition to concerns about violations of privacy and decisions about jurisdiction, cloud providers have another burgeoning problem on their hands: contributory liability. Online auction site and cloud provider eBay recently defended itself against a claim by Tiffany Inc. ("Tiffany") for contributory trademark infringement.[22] Tiffany alleged that several of eBay's users were using the site to sell counterfeit Tiffany merchandise with the Tiffany mark and that eBay should be liable for these actions by its users. In Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93 (2nd Cir. 2010), the district court utilized the Inwood test to determine eBay's contributory liability, the first time that the Inwood test was applied to an online marketplace. Under Inwood, a service provider is liable for contributory trademark infringement if one of two conditions is met: (1) the provider "intentionally induced another to infringe a trademark," or (2) the provider continued to supply its services to a user who it knew or had reason to know was infringing on

[15] Roger Smith, *Computing in the Clouds,* http://www.questia.com/library/journal/1P3-1864072981/computing-inthe-cloud (last visited Mar. 2, 2014).

[16] European Union Privacy Directive 95/96/EC O.J. (L.281) 31. *available at* http://searchsecurity.techtarget.co.uk/definition/EU-Data-Protection-Directive (last visited Mar. 3, 2014) [17] Health Insurance Portability and Accountability Act of 1996.

[17] Lisa J. Sotto "Privacy and Data Security Risks in Cloud Computing", 15 Electronic Com & L. Rep. (BNA) 186, 187 (2010).

[18] Lin Grimes & Simmons "Where Is the Cloud? Geography, Economics, Environment, and Jurisdiction in Cloud Computing available at http://www.uic.edu/htbin/cgiwrap/bin/ojs/ index.php/fm/article/view/2456/2171. (last visited Mar. 1, 2014).

[19] Lisa J. Sotto, Privacy and Data Security Risks in Cloud Computing, 15 Electronic Com. & L. Rep. (BNA) 186, 187 (2010).

[20] Mass. Gen. Laws Ann. Ch. 93 H & 2 (West Supp. 2010).

[21] Mark L. Austrian, International Cloud Computing Meets U.S.E-Discovery, available at http://www.kelleydrye.com/publications/client_advisories/0865 (last visited on Mar. 1, 2014).

[22] Tiffany (NJ) Inc. v. ebay Inc., 600 F.3d 93 (2d Cir 2010).

trademarks.[23] Tiffany asserted that eBay was liable under the second provision because Tiffany brought the infringement to eBay's attention and eBay certainly knew or should have known that users were selling counterfeit items on the site. The district court determined that eBay's generalized knowledge of infringement did not trigger the second provision of the Inwood test because eBay did not have knowledge as to specific incidents of infringement. However, a recent case from the U.S. District Court for the Northern District of California resulted in an opposite decision to that of Tiffany. In August 2009, Louis Vuitton Malletier, S.A. ("Vuitton") prevailed in an action against internet service provider Akanoc Solutions, Inc. ("Akanoc") for contributory infringement of Vuitton's trademarks and copyrights.[24] Akanoc's services included the rental of server space, IP addresses, and bandwidth to foreign resellers of the same services, who then resold the services to companies that sold counterfeit Vuitton items. Vuitton claimed that the defendants had been placed on notice of the infringing activities many times and had failed to discontinue the provision of services to the offending companies. The court in Louis Vuitton Malletier, S.A. v. Akanoc Solutions, inc. applied the Inwood test, with the determinative issue being whether Akanoc knew or should have known of the infringement.[25] Ultimately, the jury awarded Vuitton $ 32.4 million as statutory damages for the contributory infringement.[26]

The obvious question becomes: why were the judgments in these two cases are so different? Apparently, despite their similarities, the outcomes of these two cases of contributory liability for infringement turned largely on the jurisdiction in which the case was heard. The court in Tiffany determined that the warnings that eBay got from Tiffany gave eBay only generalized knowledge of infringement, whereas the court in Louis Vuitton found that Vuitton's letters to Akanoc were sufficient to find that Akanoc knew or should have known of specific incidents of infringement.[27]

D. Integration and service level issues

The data centres of cloud service providers are located in various jurisdictions and all the information of individuals and organizations are spread across the world and needs to be integrated. If the integration is not made, it will be a hurdle for individuals and organizations to get full access to their files. It is so often that the infrastructure of a customer is not compatible with the applications provided by the cloud service provider which as a result will have an impact on the working of cloud computing and the whole purpose of cloud computing gets defeated in the first place.

From a single service provider, multiple customers can have access to cloud services. The level of service can vary from provider to provider, the organizations have to make sure that the services given to them by a cloud service provider are right on time and the response is quick, this is done because the data centres are located in different jurisdictions and it will be hard for any organization to commit to cloud computing when the services given to them will not be guaranteed.

Cloud computing services are very easily available online and any individual or organization can take up the service by accepting a legal contract offered by the service provider. In most cases, the contracts favour

[23] Inwood Labs. Inc v. Ives Labs., Inc., 456 U.S. 844, 854 (1992).

[24] Louis Vuitton Malletier, SA v. Akanoc Solutions, Inc., No. C 07-03952 JW, 2009 WL 3062893.

[25] Brad R. Newberg, Louis Vuitton: A potential Game- Changer for Contributory Infringement Liability, Intell. Prop & Tech. Alert (Holland & Knight, McLean, Va.) available at http://www.lexology.com/library/detail.aspx?g=611614a0cff6-42c9-bd05-bd1719d64e1a (Visited on March 1, 2014).

[26] Louis Vuitton Malletier, SA v. Akanoc Solutions, Inc., No. C 07-03952 JW, 2009 WL 3062893.

[27] Bruce Goldner, Stuart D. Levi & Rita Rodin Johnston, ISPs Immunity from Contributory Infringement Not Abcolute, Skadden available at http://www.martindale.com/internet- law/article_Skadden-Arps-Slate-Meagher-flomLLP_804278.htm (last visited Mar. 1, 2014).

the service provider instead of securing the interest of the customer for the value he paid for the services offered to him. The scope of negotiation is restricted to making very little or no changes to the terms and conditions on which the customer affixed his signature agreeing to the contract. The contracts barely acknowledge or give any guarantee of data protection of a customer or also any backup, security, etc. The contracts generally have a saving clause and give a clean chit to the service provider for any kind of liability arising out of such a situation, wherein any case the customer is at a loss and the contract stays in the favour of the service provider.

6. Laws regarding Cloud Computing Law in different countries:- 1. European Union (EU)

In EU: Directive 95/46/EC of the European Parliament and of the Council of the European Union (of 24th October 1995)[28] - on the protection of individuals concerning the processing of personal data and on the free movement of such data; applicable to cloud computing as well. The directive is very comprehensive, covering as many questions like who is the controller of data, what the scope of authority of sub-processors is, and what happens when data is transferred outside the EU. Cloud computing emphasizes the reduction in the level of direct control over data; while the EU legislation talks volumes about keeping control of data.

2. United States (Federal and State Laws)

In the United States the Act of Stored Communications (Electronic Communications Privacy Act, 1986)[30] - a regulation that deals with intentional and compelled discovery of "stored wire and electronic communications and transactional records" held by third-party internet service providers (ISPs). Also, The Health Insurance Probability and Accountability Act, (HIPPA) of 1996 enacted in the United States contains a 'privacy rule' that controls, utilizes and leakage of Protected Health Information (PHI) and instructs that practical steps be taken to ensure the privacy of communications with individuals. The Financial Privacy Rule of Gramm–Leach– Bliley Act of 1999, compels financial organizations to present each customer with a privacy notice that must describe the data collected about the consumer, where that data is shared, how that data is used, and how that data is protected.

3. China

China's approach to Cloud Computing and data protection is highly regulatory, with stringent requirements that impact cloud providers both foreign and domestic:

Cybersecurity Law:[29] Enacted in 2017, this law requires "critical information infrastructure" data to remain within China's borders if it involves national security, public interest, or other critical areas. Cloud providers operating in China must comply with localization requirements, with extensive security protocols, periodic security audits, and risk assessments.

Personal Information Protection Law (PIPL):[30] Implemented in 2021, PIPL outlines the rights of Chinese citizens regarding their personal data, including the right to access, correct, and delete data. The PIPL also mandates that certain personal data be stored locally, with strict limitations on cross-border data transfers. Foreign cloud providers processing Chinese data must demonstrate that overseas data transfers meet security standards or face penalties, which can reach up to 5% of annual global revenue.

[28] European Commission, "EU-U.S. Privacy Shield", https://ec.europa.eu/info/law/law-topic/data-protection_en [30] H.R. Con. Res. 4952, 99th Cong. (1986) (enacted).
[29] China Cybersecurity Law (2017), http://www.npc.gov.cn.
[30] Personal Information Protection Law (PIPL), http://www.npc.gov.cn.

7. Cloud Computing in India:

Growth of Cloud Computing in India

India's Cloud Computing Market size is estimated at USD 17.87 billion in 2024 and is expected to reach USD 43.66 billion by 2029, growing at a CAGR of 19.57% during the forecast period (2024-2029).[31]

As India shifts from an emerging market to a developed economy, advanced technology is poised to play a pivotal role. Given the vastness of India's digital populace and the swift ascent of its digital economy, there is an urgent need for an expanded network of data centres. In this landscape, cloud computing in India has shifted from merely facilitating operations to actively driving innovation, flexibility, and business growth.

The Indian government's push toward a Digital India initiative is accelerating the embrace of cloud computing. Programs such as the National e-Governance Plan (NeGP) and the Government Community Cloud (GCC) amplify the demand for cloud services. The proliferation of startups and small and medium enterprises (SMEs) in India fuels the demand for cloud services as these companies seek cost-effective, scalable, and flexible IT solutions. In June 2024, Bharti Airtel, a telecom service provider, partnered with Google Cloud in a longterm collaboration to provide state-of-the-art cloud solutions to businesses throughout India.[32] This strategic alliance aims to hasten the adoption and modernisation of cloud services for Airtel's clientele. As a result of this partnership, Airtel will deliver a range of advanced cloud offerings from Google Cloud to its diverse customer base, which includes more than 2,000 large enterprises and a million burgeoning businesses.[33]

Further, in January 2024, Digital Realty, a worldwide leader in cloud- and carrier-neutral data centre, colocation, and interconnection solutions, inaugurated its inaugural data centre in India.[34] Situated on a sprawling 10-acre campus in Chennai's industrial and manufacturing hub, the facility boasts a robust capacity, supporting up to 100 megawatts of critical IT load.[35] This launch marks a pivotal expansion for Digital Realty, reinforcing its commitment to addressing the global surge in digital transformation demands.[36]

Despite the rapid adoption of cloud computing, data privacy and security remain significant challenges. Companies are cautious about migrating sensitive data to the cloud due to concerns over data breaches and compliance with local regulations.

Legal Framework of India: -

The legal system in India faces a myriad of complexities in navigating the challenges posed by technological advancements, particularly in light of the rapid growth of the internet and its pervasive influence all over the world. Time and again technology diminishes the necessity for physical

[31] Mordor Intelligence; India Cloud Computing Market Size & Share Analysis - Growth Trends And Forecast (2024 - 2029) available at Source: https://www.mordorintelligence.com/industry-reports/india-cloud-computing-market.
[32] Mordor Intelligence; India Cloud Computing Market Size & Share Analysis - Growth Trends And Forecast (2024 - 2029) available at Source: https://www.mordorintelligence.com/industry-reports/india-cloud-computing-market
[33] Mordor Intelligence; India Cloud Computing Market Size & Share Analysis - Growth Trends And Forecast (2024 - 2029) available at Source: https://www.mordorintelligence.com/industry-reports/india-cloud-computing-market
[34] Mordor Intelligence; India Cloud Computing Market Size & Share Analysis - Growth Trends And Forecast (2024 - 2029) available at Source: https://www.mordorintelligence.com/industry-reports/india-cloud-computing-market
[35] Mordor Intelligence; India Cloud Computing Market Size & Share Analysis - Growth Trends And Forecast (2024 - 2029) available at Source: https://www.mordorintelligence.com/industry-reports/india-cloud-computing-market
[36] Mordor Intelligence; India Cloud Computing Market Size & Share Analysis - Growth Trends And Forecast (2024 - 2029) available at Source: https://www.mordorintelligence.com/industry-reports/india-cloud-computing-market

communication in the formation of important relationships in legal terms between the parties. Hence, it is up to the legal system to settle the code of behaviour to be followed by such parties in sustaining such legal relationships. Until the Information Technology Act, of 2000 was enacted, there was no law concerning the usage of computers, computer systems and computer networks, as well as data and information in an electronic form in India. The primary aim of the Information Technology Act 2000 is to present legal gratitude to e-commerce, which involves the use of electronic means of communication and storage of information, and to facilitate the electronic filing of documents with government agencies. The Act has extra-territorial jurisdiction so it also covers offences committed outside India.

The IT Act deals with a range of computer-related works such as digital signatures, electronic governance, electronic records, regulation of certifying authorities, duties of subscribers, cyber regulations, the appellate tribunal, etc., and also offers for legal identification of electronic documents and transactions, the admissibility of electronic data/evidence in a court of law, penalty for cybercrimes, and the institution of an appellate tribunal and advisory committee for regulating cybercrimes and regulations regarding the maintenance of electronic records. Nonetheless, the Act also has numerous grey areas, i.e. it does not grant a shield against copyright infringement, defence of domain names, taxation on e-transactions, stamp duty payable and the jurisdictional aspect of e-contracts. However, efforts are being made through a number of amendments to do away with the ambiguities.

The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules of 2011 were notified by the Government of India, for the protection of sensitive personal data or information of individuals or organisations by the entity who possesses, deals with or handles such data in a computer resource owned, controlled or operated by it.[37] However various provisions of the Rules of 2011 do not apply to entities providing services under a contractual obligation with any other entity located extraterritorially unless such entity ensures the same level of data protection as laid down in the Rules.[38] So a cloud computing service company, before trading with "sensitive personal information" [39] having a link to India, has to make sure to be in observance with the Rules as any non-compliance would invite penalties, and imprisonment in the case of any breach of contractual obligations under the Information Technology Act 2000. Hence, cloud service companies have to make sure that both the rules and terms of the contract entered into with the customers are complied with.

The IT Act of 2000 enforces a compulsion on a corporate body to provide for a privacy policy and disclosure of information. The entities dealing with any "sensitive personal data or information", or any other personal information, shall provide a privacy policy published on their website. The corporate body has to make certain that such personal data is available at all times to its clients.

When it comes to the security of the information stored, the companies are supposed to make sure that they protect such information by implementing the "Reasonable Security Practices and Procedures". This states that the International Standard on "Information Technology - Security Techniques - Information Security Management System -Requirements" has been adopted by the government of India. Any corporate body implementing such standards is said to have obeyed the said act with regard to practical

[37] Reema Patil, Notification of the Rules with respect to Protection of Sensitive Personal Data and Information under the Information Technology Act, 2000, available at http://www.narasappa.com/resources/InformationTechnologyRules.pdf (last modified Jan. 14, 2014).

[38] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Gazette of India, part II section 3(1), R.7 (Apr. 11, 2011).

[39] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Gazette of India, part II section 3(1), R. 3 (Apr. 11, 2011).

security practices and procedures. The law also requires a complete information security programme, standard information security plans including the managerial, technical, and operational charge of security, and physical actions that are proportionate with the secluded information possessions and which obey reasonable security exercises and standards.

Rule 6 of the said act sets down the mode in which the data can be revealed to a third party. It asserts that no leakage of any sensitive personal data shall be made without the former approval which has been contractually agreed between companies by the corporate.[42] No data shall be passed on by the corporate to any third party unless such third party has acted in accordance with the minimum security criteria as specified under the rules. It specifies that government outfits can collect any sensitive information, for the purpose of authentication of identity, or for prevention, detection, investigation, prosecution and punishment of offences.[43] Nonetheless, any individual who in pursuance of his powers conferred by the Act gains access to any data and reveals such information without the approval of the person concerned, triggering wrongful damage to such a person, shall be likely to have proceeded for imprisonment, which may extend to two years, or to a fine, or to both.

[42] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Gazette of India, part II section 3(1), R. 6 (Apr. 11, 2011).

[43] 27 Rahukar, The Information Technology Rules, 2011 CLUB HACK MAGAZINE, http://chmag.in/article/apr2011/information-technology-rules-2011 (last visited Jan. 12, 2014).

One of the foremost loopholes of cloud computing services in India is that there is no precise law prevailing over the possession of data on a cloud. Generally, the service-providing companies possess the data unless it has been contractually agreed between the parties. This depicts the customer's information to various perils as the rights of such data are vested with the cloud provider. Under the Information Technology Act of 2000, a cloud service provider is not accountable for any third-party data made available by him, if he shows that such infringement or offence was committed without his awareness or that he has exercised due diligence as may be prescribed by the Government for the prevention of such offence.[40] In the Information Technology Act, of 2000, amended section 10A has been placed which says that a contract which has been made electronically shall not be regarded to be unenforceable. Yet, there is still elusiveness as to if an electronic contract is to be stamped, as the process of payment of stamp duty as envisaged under the Stamp Act is not possible in cases of electronic contracts unless they are printed.

In particular situations, the parties entering into a contract have a choice to prefer the law which shall preside over them in the case of any difference of opinion arising in the future. But this is not the same in all matters. As a result, the applicable law and the authority of the court remain a loophole as the contract entered into between the parties lacks clarity on such matters.

8. Conclusion:

Cloud computing offers remarkable advantages for data storage, processing, and accessibility, enabling organizations and individuals to scale their resources efficiently and reduce expenses associated with on-premises infrastructure. In India, where digital transformation is accelerating, cloud computing holds transformative potential to support government initiatives, drive business innovation, and expand digital services to the wider population. However, this growth is accompanied by noteworthy challenges, as the

[40] The Information Technology Act, No. 21 of 2000, INDIA CODE

current legal framework has yet to catch up with the complexities and risks associated with cloud technology. The current legislation, the Information Technology (IT) Act, of 2000 [41] provides a fundamental regulatory framework concerning electronic records, digital signatures, and cybercrime, but it is insufficient to address the nuanced requirements of cloud computing, such as data privacy, jurisdictional clarity, cross-border data flow, and accountability for cloud service providers.

With global regulations such as the General Data Protection Regulation (GDPR) setting high standards for data privacy, Indian organizations engaged in international trade and business or data exchange must navigate the complexities of compliance, which further underscores the need for India to develop a cohesive regulatory approach that aligns with international norms.

To maximize the potential of cloud computing while protecting users' rights and data integrity, India needs to implement a dedicated, modernized legal framework that addresses the specific challenges of cloud technology. This framework should define clear rules on data privacy, security protocols, cross-border data transfers, and the liability of cloud providers in case of breaches or service disruptions. The framework needs to mandate data localization standards where necessary, clarify the jurisdictional scope for international data handling, and establish protocols for data portability and consumer protection. This will provide both users and businesses with the confidence needed to fully embrace cloud solutions, supporting India's goal of a robust digital economy.

Furthermore, adopting best practices for data security, instituting clearer guidelines for service-level agreements, and ensuring that cloud providers adhere to transparency and accountability standards will help mitigate risks. Aligning India's cloud regulations with global data protection standards, such as GDPR, can provide a competitive advantage to Indian businesses and facilitate smoother cross-border operations. The harmonization of regulations would also strengthen India’s position as a global technology leader, fostering trust and reliability in Indian cloud services on the international stage.

In conclusion, cloud computing has the potential to drive substantial growth and innovation within India’s digital economy. However, its successful adoption will require a comprehensive and futureoriented regulatory framework that addresses legal, security, and jurisdictional issues unique to cloud computing. By establishing stronger, clearer regulations, India can create a more secure and predictable environment for cloud technology, which would not only support digital transformation domestically but also enhance the country’s competitiveness in the global digital marketplace. This will empower Indian organizations to leverage cloud solutions confidently, fostering innovation, economic growth, and a secure digital infrastructure that serves both national and global interests.

[41] The Information Technology Act, 2000 (ACT NO. 21 OF 2000) w.e.f:- 17th October 2000, vide notification No. G.S.R. 788 (E), dated 17th October 2000, see Gazette of India, Extraordinary, Part II, sec. 3(ii).