Hindawi
Security and Communication Networks
Volume 2023, Article ID 9763838, 1 page
https://doi.org/10.1155/2023/9763838

Retraction

Retracted: Cloud Computing: Legal Issues and Provision

Security and Communication Networks

Received 10 October 2023; Accepted 10 October 2023; Published 11 October 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. S. Saini, D. K. Saini, P. Gupta, C. S. Lamba, and G. M. Rao, "Cloud Computing: Legal Issues and Provision," *Security and Communication Networks*, vol. 2022, Article ID 2288961, 13 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 2288961, 13 pages
https://doi.org/10.1155/2022/2288961

Review Article

Cloud Computing: Legal Issues and Provision

Jaskaran Singh Saini,[1] **Dinesh Kumar Saini**,[2] **Punit Gupta**,[2] **Chhattar Singh Lamba**,[3] **and G. Madhusudhana Rao**[4]

[1]*Department Business Administration, Manipal University Jaipur, Jaipur, India*
[2]*Department of Computer and Communication Engineering, Manipal University Jaipur, Jaipur, India*
[3]*Department of Computer Science and Engineering, Manipal University Jaipur, Jaipur, India*
[4]*Bule Hora University, Bule Hora, Ethiopia*

Correspondence should be addressed to Dinesh Kumar Saini; dineshkumar.saini@jaipur.manipal.edu

Received 9 May 2022; Revised 20 June 2022; Accepted 27 June 2022; Published 1 August 2022

Academic Editor: Mukesh Soni

Micro, Small, and Medium Enterprises (MSMEs) are gradually adopting cloud-based solutions using Information, Communication, and Technologies (ICT). Due to the lack of awareness regarding the legal challenges arising from jurisdictional issues of the Cloud Service Provider (CSP), MSMEs often get entangled in expensive litigations. The paper throws light on such legal conflicts and proposes new innovative ways (such as bilateral treaties, US CLOUD Act, Mutual Law Assistance Treaties, and In-house Capability) to tackle the same. Any domestic law governing data privacy must align with the globally acceptable standards prevalent in the international perspective. In the era of industrial revolution 4.0, data is the new oil, wherein any country having control and understanding of the intersectoral dimensions of the cloud-based data indeed gains an edge over the competition. Due to the prominence of the global private sector in providing local public services, there is a need for government authorities to take flexible approaches while formulating domestic laws in the realm of cloud computing.

1. Introduction

Cloud computing is the future of the NextGen computing systems in the world. The word "cloud" itself relates to any formation over and above Earth but near enough to influence the Earth's atmosphere. A report published by Market and Markets estimates the cloud computing market size to increase from $445 billion in 2021 to $974 billion by 2026. Amidst the COVID-19 wave, work-from-home (WFH) culture gained wide acceptance, and there seems to be a tectonic shift towards digitalization of all the essential physical services. Under such circumstances, cloud computing is predicted to achieve a CAGR of 16.3% [1]. Cloud Computing enables decentralized data processing with the centralized storage of data. Such an approach helps mitigate the need to carry storage devices along with the computer. This further lowers the cost of computing devices and makes digital devices much more affordable [2]. The data is collected and stored at the central location aids the availability of data on-demand as and when required. Nowadays, Cloud Computing is the backbone of the infrastructure deployed to deliver public services worldwide. The data stored on the cloud is scalable, and hence can be used by various government departments to provide public services directly at the doorstep of the end-user [3].

India is home to approx. 7.8 crore Micro, Small, and Medium Enterprises (MSMEs), and are registered on the Udyam Registration Portal with an annual contribution of 30% to the GDP. At least 11 crore people (in 2020) are employed in the MSME sector, thus showcasing a colossal bulwark of employment generation in the Indian economy [4]. Moreover, 99.55% of the MSMEs are Micro and Small Enterprises and contribute 40% to total exports [5]. MSMEs in India are said to be the goldmine of the traditional knowledge economy, which has preserved old customary methods and practices in several sectors such as textile, artworks, and paintings. The meticulous efforts by the government in the form of Make in India, Emergency Credit

Line Guarantee Scheme, Zero Defect-Zero Effect (ZED) certification, etc., have rejuvenated the sector in the distressing times. The pandemic has proven a disguised opportunity, providing MSMEs impetus to adopt digital presence, thus enhancing their outreach manifolds transcending geographical boundaries. For instance, 72% of the payments are done using digital mode vis-à-vis 23% of cash transactions [5].

Gradually, businesses are rapidly adopting the cloud-based system for their global outreach and meeting the statutory objectives of the Digital India Scheme. Information, Communication, and Technology (ICT) interventions pave the way for doorstep delivery of goods and services by eliminating or limiting the role of intermediaries. It enables the MSMEs operating in far-flung rural areas to market their products directly to the consumers at a competitive price, thus facilitating a globalized presence of localized products [6]. The adoption of cloud computing is a capital-intensive venture from the perspective of budding MSMEs, such as start-ups or enterprises reaching the breakeven point in their business cycle. Indian Information Technology (IT) companies' excellence is widely acknowledged in providing competitive IT services to their clients primarily located in the USA and European nations. Due to economies of scale, the per Giga Byte (GB) cost of data in India is among the lowest in the world, e.g., $0.68 average cost per GB of data [7]. Such conditions are conducive to the MSMEs' ready adoption of cloud-based systems. Considering MSMEs surmount technological and financial constraints with requite governmental support and handholding by several e-commerce giants [8]. Still, there would be immense legal complexities involved while utilizing cloud-based services across the globe. In the realm of Data Economy, it is crucial to precisely determine the ultimate ownership of the user's data amidst the global tussle between Data Protection Laws and ICT legislations.

MSMEs have a multisectoral presence in India, collaborating at different production levels with their counterparts or non-MSMEs. The blend of centralized control of decentralized processes is the forte of cloud-based transformation. It may be in the form of cost-saving, ease of use, sharing and collaboration, security and privacy, etc. But the complexities arising out of the sporadic location of the cloud servers (discussed under Section 7), and the statutory obligation of domestic data protection laws, tend to escalate the litigation cost for the MSMEs [9].

The paper discusses the legal challenges that MSMEs would encounter during the adoption of cloud-based systems. The data stored on the cloud is cross-sectoral and can be instantly accessed from varied geographical locations. Hence, the propensity of legal bottlenecks tremendously multiplies too. In the later section of the paper, various jurisdictional issues and the proposed solutions are deliberated in detail. The endeavor is to make MSME aware of legal challenges arising out of cloud-based storage and suggest the policymakers take corrective legislative and executive remedial steps accordingly.

Cloud-based computing in India has epitomized in the form of JAM Trinity [10], a govt flagship initiative to provide three basic services, i.e., (i) Jan Dhan (access to bank accounts for all), (ii) Aadhar (identity proof), and (iii) Mobile (communication), to all its citizens. The scheme aims at digitalizing and integrating the public data under one umbrella, thereby paving the way for more comprehensive financial inclusion. By using cloud-based infrastructure, the scheme successfully identifies the beneficiaries and helps the government directly transfer the subsidy (using Direct Benefit Transfer) amount into the bank account of citizens, eliminating the multiple layers of intermediaries. Such Information, Communication, and Technology (ICT) solutions help policymakers weed out the unintended beneficiaries availing subsidies to the tune of Rs. 3.17 lakh crore (as per the Budget Estimates of 2022–23) [11] and ensure timely transfer of social security benefits. Figure 1 shows how cloud-based data can deliver various public services by the govt and private service providers.

Cloud-based services are seamless but broadly can be categorized as follows:

(i) Software as a Service (SaaS): the software is used to provide any particular service. Any company or service provider is designed explicitly with customizations to provide any service, e.g., the AarogyaSetu app, Gmail, and Google Docs [12].

(ii) Infrastructure as a Service (IaaS): service provider leases its infrastructure or creates an infrastructure that can be used to deliver any kind of public or private service, e.g., Amazon's Elastic Compute Cloud (Amazon EC2) [13].

(iii) Platform as a Service (Paas): a dedicated platform is created to provide any specific kind of service, e.g., Netflix and Microsoft Azure [14].

The type of service, i.e., SaaS, IaaS, or PaaS, does not operate in silos; instead, more than one can be bundled with another while catering to the customer's need. For instance, Dropbox, which provides cloud storage, utilized Amazon's EC2 IaaS. Similarly, PaaS can use the IaaS of another service provider [15].

2. Why It Is Required?

The Govt of India (GoI) launched its indigenous cloud named "MeghRaj" in 2014 to provide e-services to its citizens and strengthen the reach of Information, Communication, and Technology (ICT) in India [16]. With the increasing penetration of e-services, the demand for cloud computing has already risen to manifolds, offering tremendous opportunities for India in the near future. The Indian services sector is the pioneer in providing affordable and reliable software-based solutions across the globe. But in the realm of cloud storage, few global players are dominant such as Amazon Web Services, Google Cloud, Apple's iCloud, Microsoft's OneDrive, etc. Many smartphones or digital device manufacturers enter into an agreement with the mentioned global cloud storage giants for using their infrastructure to store customers' data. This leads us into a grey area compounded by the jurisdictional conundrum.

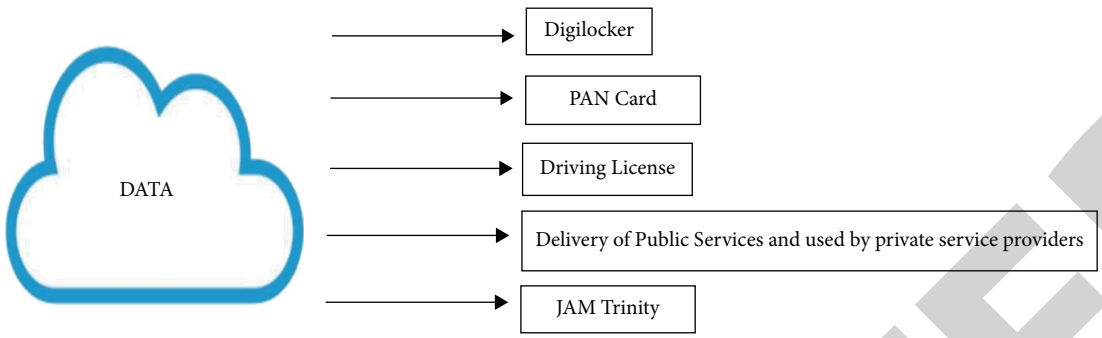

Figure 1: Cloud and its linkages.

The 21st century is the era of data privacy wherein heated debates over the storage and ownership of public data are a common sight. The cloud-based storage further gets complicated because the service providers are located in diverse geographic locations. In legal terms, it becomes challenging to define the roles and responsibilities of multiple stakeholders involved in the cloud computing infrastructure. For instance, the data of an Indian user may be stored on a smartphone manufactured in South Korea. The smartphone manufacturer may further use the cloud services of a US-based company that may host its data servers in European nations. In this simple example, it can be seen that four geographical locations are involved in storing the data of a single Indian user. In the case of any data breach, it becomes a judicial nightmare to clearly define the accountability matrix for various stakeholders. The service providers often exploit the legal ambiguity in cloud storage, due to which many customers lose their data entirely or leak it into the public domain. The Industrial Revolution (IR) 4.0 is based on automation, cyber-physical systems, the Internet of Things (IoT), and Cloud Computing, enabling the use of smart technologies in every sphere of life [17]. Hence, the clarity in legal aspects of modern technology in tandem with its influence on the delivery of public services is the need of the hour.

Bureaucracy, an organizational structure model, proposed by Max Weber in the late 19th century, has gained wide acceptance in the government functioning across the globe. The model has been widely criticized for highly relying on documentation and rules rather than serving the genuine public cause in the form of Red Tapism (a phenomenon of accumulating piles of files with red ribbons on the top of the desk of officers leading to immense delays in decision making by the governments). Cloud-based services are the best possible way to confront the Red Tapism malady by making public services more transparent and accessible to beneficiaries. On the other hand, the policymakers can map all the citizens and associated services in real-time, thus reducing the financial burden on the public exchequer. Moreover, the citizens can hold the state and services accountable through ICT-based grievance portals hosted on the cloud servers. Hence, cloud-based services are mutually beneficial for both the citizens and the state in achieving the goal of cost-effectiveness and bringing the government under sunlight (famously remarked by Louis Brandeis, an American Justice, Sunlight is the best disinfectant, i.e., transparency of public policy is essential to arrest corruption).

Cloud computing is characterized by five attractive benefits companies can leverage in delivering cost-effective services in the long run [18]. These include the following:

(i) On-demand self-service helps the customers avail services without a third party's interference. The end-user can choose the type of service as per the need or, in some cases, take advantage of customized cloud features.

(ii) Broad cloud network provides universal access to all users across the globe in real-time. Due to the record download speed of the Internet, the cloud-based storage can be as quick as the localized SSD (Solid State Device) on the computer.

(iii) Resource pooling aids the Cloud Service Provider (CSP) to reap economy of scale benefits and provide budget cloud services. It also increases IT hardware and infrastructure utilization efficiency, thereby lowering environmental carbon emissions and power consumption.

(iv) Rapid elasticity allows the customer to utilize the cloud data on-demand as and when required. Due to the centralized storage, the users can simultaneously consume the data in different devices located at diverse locations.

(v) Measured service permits CSPs to implement a Pay-as-you-go model for their customers.

3. Objective of the Study

The paper aims to identify the legal and jurisdictional challenges encountered by the Cloud Service Provider (CSP) and to recommend a suggestive policy approach. Other relevant issues related to cloud-based data are identified in the course of the literature review and presented as a summary in Table 1 of the paper.

4. Different Models

The cloud-based services can be deployed using three basic approaches. Figure 2 shows the types of models.

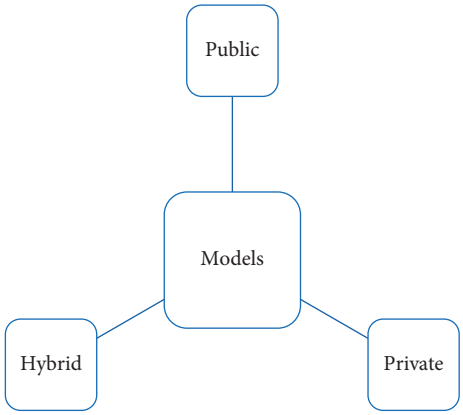

Figure 2: Types of models.

(1) Public: under this model, a third party operates and owns the cloud services. It is a cost-effective way of implementing cloud-based services as the maintenance and management of the cloud infrastructure are not borne by the end-users or organizations. The model users can benefit from the Pay-as-you-go approach, allowing them to choose plans best suited for their needs. Due to economies of scale, Cloud Service Providers (CSP) can offer cloud-based services bundled with the other services on their platform in the form of a package, e.g., Apple provides 5 GB of free iCloud storage to their customers. And sometimes, the benefits are offered free to a limited extent, e.g., Google offers free 15 GB of storage to every customer; post the free limit, customers are charged but at very reasonable rates. For instance, MeghRaj (an Indian government cloud server) involves various CSPs from the subnational level and other private CSPs to come together to deliver e-services [16]. The only downside of the public model is the data privacy and security concerns, as the complete cloud infrastructure is owned and maintained by a third party [19].

(2) Private: this model helps an organization own, operate, and manage complete cloud-based infrastructure, specifically tailored to meet the needs of a particular business entity. The data servers, hardware, and software are under the control of the private player, and cloud-based services are not open to public use. It offers an opportunity for the organization to design a customizable cloud with a varied degree of personalized features. Most of the highly sensitive government's classified data utilize the private cloud, providing access to only limited users as per the requirement. However, it is an extremely capital-intensive proposition as a single private entity manages the entire cloud infrastructure. As the cloud data is restricted to few users, this model is less prone to legal challenges and jurisdictional issues generally associated with cloud-based data sharing [20].

(3) Hybrid: in this model, public and private services providers jointly collaborate to offer unified services. It benefits the govt or public service provider to utilize the capabilities and the expertise of the private player while ensuring privacy features of the private cloud accompanied by the scalability benefit of the public cloud. Due to its seamless interoperability among different clouds, the government can use this model to provide e-services and digitalize essential public services in the long run. For instance, there are specific laws Data Protection Directive (DPD) of the European Union (EU) [15]and the Indian Data Protection Bill [21], which prohibit the location of physical data servers outside the parent country. The hybrid model of cloud storage can aid the CSP in meeting the regulatory compliances of their clients and mitigate the litigation cost associated with the cloud data. This model is often preferred by the government worldwide as it facilitates the government to meet its divestment or disinvestment goals (in some countries). Hybrid models also enable the seamless data transition between public and private clouds with relatively fewer legal implications [22].

5. Legal Challenges

Legal challenges arise due to the involvement of various jurisdictions in the storage, processing, and sharing of cloud-based data [23]. Further, the data in different countries are governed by country-specific laws and regulations and may being consistent with data privacy laws of other countries (e.g., GDPR vs. USA CLOUD Act is discussed later). Let us discuss in brief the various legal challenges that can impede the path of cloud computing globally: Figure 3 shows the types of legal challenges.

(1) Liability: the data stored on the servers might be the intellectual property of an individual, company, or community. The cloud service provider may have the luxury of locating its servers in the location of their choice. But the ultimate liability for protecting the data rests upon the service provider itself. Here, govt can also be a service provider and hence be liable for its safe storage and authorized usage.

(2) Compliance: the service providers are obligated to comply with the law of the land where the data servers are located. The noncompliance to the regulatory framework can lead to increased legal barriers, further aggravating the time and cost overruns in implementing a particular project. Too much regulatory compliance can hamper the business prospects, thus making the business environment rigid.

(3) Copyright: the data is the intellectual property of the individual or an organization. The data breaches and theft may render the service provider of cloud-based services noncompliant with international agreements such as WTO's TRIPS (Trade-Related Aspects of Intellectual Property Rights) and may invite global sanctions [24]. Copyright infringement in modern

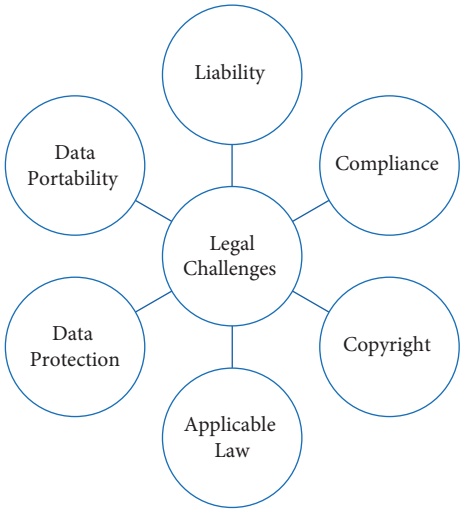

Figure 3: Types of legal challenges.

times is one of the strictest forms of legal penalties imposed by regulatory agencies worldwide.

(4) Applicable law: different kinds of data should comply with other sectoral laws cutting across various sectors and domains. For instance, accounting data in India is under Indian Accounting Standard (IAS), and data from banking institutions is under the supervision of the RBI (Reserve Bank of India). Moreover, domestic and international laws may also impose an obligation upon the service provider to disclose the individual`s data to the govt under a specific condition (as in the case of the US CLOUD Act). It becomes a balancing act for the cloud-based service provider to weave their path amidst a statutory conundrum.

(5) Data protection: on an interjurisdictional platform, the cloud-based data must conform to several data protection laws applicable to data exchange between the service provider and end-user. For instance, data of storage of a single user on the cloud may require the service provider to comply with the laws of four to five countries. The service provider can deploy various data protection techniques such as end-to-end encryption, Blockchain Technology, etc. Data protection is one of the top most priorities amidst the ongoing cyberattacks, ransomware attacks, and malware attacks on the public system, making cloud-based services vulnerable to abuse and misuse.

(6) Data portability: the data stored on servers, in general, is not standardized. In some cases, due to rapid technological upgradation, the stored data on the cloud may encounter mismatch errors. It is paramount that periodic data review is done with the stakeholder's mutual consent to avoid format-related anomalies. The data portability is all the more critical because the same data on-demand is used in different operating systems simultaneously (e.g., accessing Microsoft Excel sheets on both Android phones and iPhones).

Legal challenges exhibit a complex relationship with the jurisdictional issues (discussed in Section 7) for cloud-based data. Due to the absence of the standard legal framework for cloud servers, CSP often gets caught in a legal conundrum in the process of complying with multiple domestic laws of the participant's nations. There is an intricate association of data protection laws with the ICT laws from both national and international perspectives. At the moment, there is a lack of consensus among the developed and developing nations on how the data should be treated. For instance, three basic approaches are in the discussion, i.e., the Individualistic approach (data ownership resides with the individual), the Collectivist approach (collaborative sharing of nonpersonal data for common societal benefit), and the Community approach (akin to natural resources, it is the community which collectively owns the data) [25]. The data hosted on the cloud servers will encounter the winds of legal and jurisdictional ambiguities until the international community does not settle the data ownership challenge. Most CSPs are located in the western countries (the USA or Europe), where strict adherence to data laws is observed. The third-world nations serve as a lucrative market for the west-based cloud-service giants. Hence, to prevent the monopolization (or oligopoly) of cloud services, data governance and legal framework need a simultaneous consideration to resolve jurisdictional issues in the future.

6. International v/s National Perspective

Be it any model that provides cloud-based services; the legal implications need urgent redressal. Cloud computing has risen to a level in recent years wherein the external storage provided in personal computers and smartphone devices seems redundant. The data is said to be the new oil in the era of Industrial Revolution 4.0. Hence, the public data stored on the private or public cloud needs to be tempered with robust Data Protection statutes across the globe [17]. The data protection law can be subdivided into two categories for our better understanding: Figure 4 shows the governing principles.

(1) Domestic law: this relates to uniform country-specific laws that clearly define the roles and responsibilities of the various stakeholders involved in data-driven services. The Internet and several digital technologies have integrated various segregated paper-driven services. With every ticking second, countless gigabytes of data are generated by the users on the Internet. Such data needs a framework and guidelines for its storage on the private/public cloud, clearly defining the terms and conditions for its usage across the Internet. In the absence of domestic data protection laws, the govt has a huge opportunity cost as the data is freely available for use and misuse. India and China are the fastest-growing economies in the world, comprising approx. 37% of the world population. One can imagine the level of vulnerability with the data stored on the cloud if no checks and balances exist.

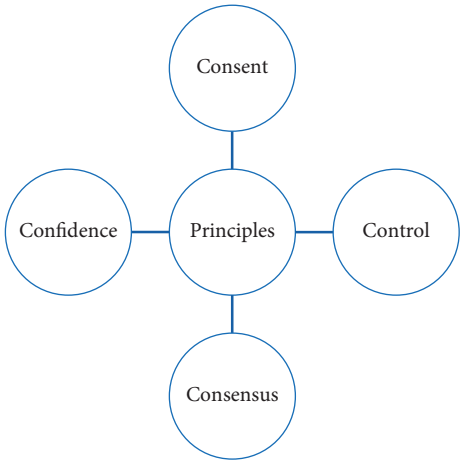

Figure 4: Governing principles.

Moreover, in the realm of cloud storage, as discussed earlier, the monopoly of the few global giants makes the situation all the more alarming. The European Union has passed its infamous General Data Protection Regulation (GDPR) Act [26], which has become a gold standard for data regulation worldwide. Other countries have started imitating the GDPR or similar laws to protect their domestic data. We need to draw a line between public and private data while understanding the legal implications of cloud computing. The public data has the direct supervisory control of the govt of the day. Additionally, govt is also responsible for its usage, sharing, and processing while providing various public services. The coercive measures can be used by the govt or any regulatory agencies wherever public data is concerned. On the other hand, private data is the sole property of the individual citizen, and they need ultimate authority to permit its usage. The policies governing private and public data should not be painted with the same brush following the One Size Fits All Approach. Democratic principles must be at the forefront while formulating statutes concerning private data. Below are some of the principles that should form the basis of any regulation.

(a) Consent: the private/public service provider needs to take the prior authorization of end-users before utilizing their cloud-based data for any other purpose. Even the govt or data regulator must collect a minimal amount of data while providing public services. Every individual has the Right to be Forgotten whenever the data is floated in the public domain [21]. The govt should try to formulate due procedures and regulations wherein the citizen can be monetized (if possible) in case private agencies use their data. Monetizing data can act as a stable source of revenue for the government by providing data mining companies limited access to public cloud-based data [27].

(b) Control: the country's citizen has the right to own and use their data. In India, the Right to Privacy is recognized as a fundamental right under Article 21 of the Indian Constitution. Following the spirit of this principle, the Indian Data Protection Bill 2018 emphasizes Data localization, mandating that the data of the Indian citizens need to be stored on servers inside India's territory [21]. Data localization is a very debatable argument from the point of view of anonymity that the Internet offers to global cloud-based companies. The control over the personal data stored on the cloud forms the bedrock of any Data Protection Law worldwide. The way to address legal implications arising from cloud-based data is discussed later [28].

(c) Consensus: any policy concerning cloud computing should be done with the concurrence of the various stakeholders. As done in China and Vietnam Data Protection laws, awarding sweeping powers to law enforcement agencies to manage cloud-based data under certain conditions without consent (as done in China and Vietnam Data Protection laws) is sheer non-democratic governance. Even the Indian Draft of the Data Protection Bill [21] is often criticized for allowing executives to supervise cloud-based data without judicial oversight. The data is saved on the cloud but used by many software in various forms (such as Health Data and Financial Data) without adhering to any common standard. The consensus principle also highlights the need for multiple data agencies to agree to a common standard for the storage and processing of cloud-based data [29].

(d) Confidence: it is an essential aspect of any regulation. The users need to have confidence and trust in the various agencies enabling fair use of cloud data. The data needs to be firewalled against any untoward virus attacks, cyber warfare, or malware, especially while storing the individuals' banking details (financial data). The public should have confidence in the laws dealing with cloud data protection and trust law enforcement agencies' abilities. To boost the citizenry's faith, the govt must ensure the democratic participation of the various stakeholders in the implementation and formulation of the guidelines. Further, the rules and framework should be consistent and clearly worded in terms of the responsibilities and obligations of the stakeholders.

(2) International law: primarily the data servers are located in temperate regions due to the relatively cool temperatures. This saves a lot of expenditure otherwise spent on the air conditioning of the facilities hosting data servers. Hence most of the data servers are usually located in European nations. In

case of a data breach, as several stakeholders are involved from different locations, it becomes challenging for legal agencies to extract accountability. Conversely, the aggrieved end-user tries to avoid expensive legal battles due to the various legal systems involved. As discussed earlier, the European Union's GDPR Act [26] is considered the gold standard in data privacy. The recent trends in global governance exhibit the elements of protectionism in their policies. There is an informal wave of antiglobalization wherein domestic growth and well-being trump global sustainable development. For instance, Make America Great Again (MAGA), Atmanirbhar Bharat [30], US sanctions on Chinese imports, etc., show how global governance is taking a U-turn and turning protectionist. Amidst such a vitriolic environment, the data stored on cloud servers may become a causality. Or the nations hosting the data servers, having technological competence in cloud-based systems, may be in an advantaged position to arm-twist global policies to their advantage. The urgent need is to clarify standards, rules, and regulations of cloud-based computing on an international basis. The principles discussed under section Domestic law, i.e., Consent, Control, Consensus, and Confidence, are relevant here. It is imperative to have a global consensus over an international organization or a commission, maybe under the aegis of the United Nations (UN), empowered to set basic guidelines for storing, processing, and sharing cloud-based data. The dispute resolution mechanism is necessary to allow different stakeholder to raise their concern. To increase the commission's credibility, the commission must have some Quasi-judicial powers to instruct the parties in their dispute settlement.

7. Jurisdictional Issues

With the advent of Big Data and its amalgamation with Cloud Computing, the storage capacity requirement and data analysis capability have reached astronomical levels. The 19th and 20th centuries were marked by technological discoveries, whereas the 21st century would be the era of Digitalizing Everything so far invented. Due to the multiplicity of digital devices aiding in the 5V's of Big Data (Volume, Velocity, Variety, Veracity, and Value), localized physical storage devices (hard drives, pen drives, CDs, etc.) are becoming things of the past. Cloud storage bridges the data sharing vacuum among myriad digital devices by enabling real-time data transfers (in Terabytes per second), taking advantage of the cutting-edge computational abilities of smart devices. The infamous physics experiment Large Hadron Collider (LHC) produces 60 TB (Terabyte) of experiential data per day and 15 PB (Petabyte) of data per annum [31]. Moreover, emerging digital technologies such as the Internet of Things (IoT), Cyber-Physical Systems (CPS), Robotics, Automation, etc., generate zillions of data per annum to be shared across the globe in real-time only be met by cloud-based storage.

The energy requirement of data servers is equivalent to the energy consumption of 25,000 homes, consuming 100–200 times more energy than a standard office. On the other hand, there is a sharp spike in the year-on-year energy consumption of the data centers, typically doubling every five years [32]. This massive energy consumption of cloud-based storage servers prompts CSPs to optimally locate their servers in different geographic locations. It helps has two essential benefits; firstly, the peak load on a particular server can be offloaded to other data centers. Secondly, CSP can avail differential power tariffs at a given point in time, thus significantly minimizing their energy costs. It might be economically viable for the CSP to distribute its servers across the globe, but on the other hand, the data stored on the cloud is governed by varying data protection laws contributes to jurisdictional issues arising out of cloud-based storage. Figure 5 illustrates the distribution of servers in different geographic locations while CSPs provide cloud services (IaaS, PaaS, or SaaS) [33].

The Cloud Client (CC) and CSP relationship is complex and depends extensively on the type of service offered. In simple terms, CC has maximum control over the cloud data and its usage in the IaaS and gradually cedes authority in PaaS and SaaS (as shown in Figure 6). Therefore, CSP has more responsibility and accountability for cloud-based data hosted on their servers in PaaS and SaaS. Further, the CSP's customization abilities for their customers and the governing data legislations of the CC and CSP determine the ultimate legal responsibility of the cloud data [34].The Service Level Agreements (SLAs) are negotiated between CC and CSPs to settle or avoid the legal implications in the future. Still, the vulnerabilities arising out of vagaries of cloud data cannot be set aside altogether. It is advised that SLAs should be comprehensively negotiated, and all the possible alternatives to data breaches and security challenges need to be addressed to the fullest satisfaction of CC by the CSPs. The cloud server exhibits no physical boundaries, and there can be possibilities wherein CSP providing IaaS is utilizing the PaaS of another CSP in the background. When the customer data is hosted on servers in a third country, the customer's data legislation/laws must address such anomalies with clarity and decisiveness. For instance, US PATRIOT Act [35] permits the enforcement officials in extreme circumstances to coerce the CSP to provide the sought confidential information of the suspect. On the other hand, European Union Data Protection Directive [15] clearly defines the data ownership of its citizens irrespective of the location of the data servers in the third world [15, 36].

To take data security and protection against misuse, the CSPs should implement Virtual Information Security and Management Systems (ISMS) along the lines of ISO/IEC 27001 [37]. The conventional ISMS aims at securing the organization's IT assets (including hardware, software, data, and infrastructure). After due discussions and deliberation with stakeholders, Virtual ISMS should be made applicable to all the cloud servers establishing definite standards and protocols for the CSPs [38]. It would create an environment

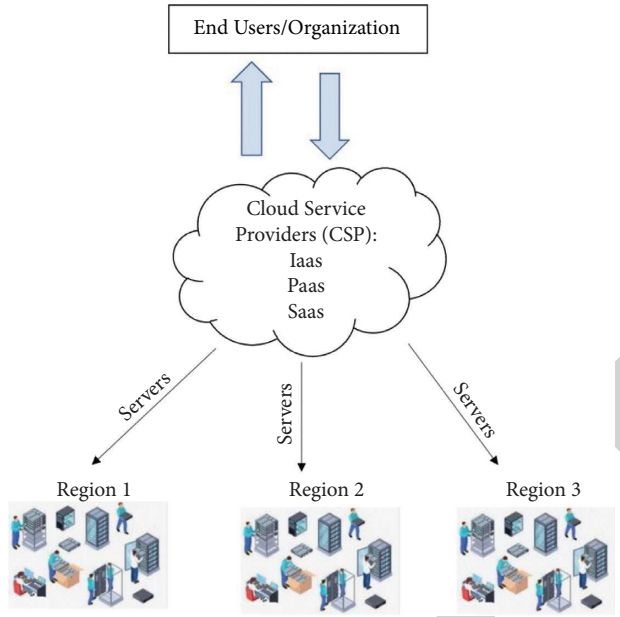

Figure 5: Interregional placement of servers.

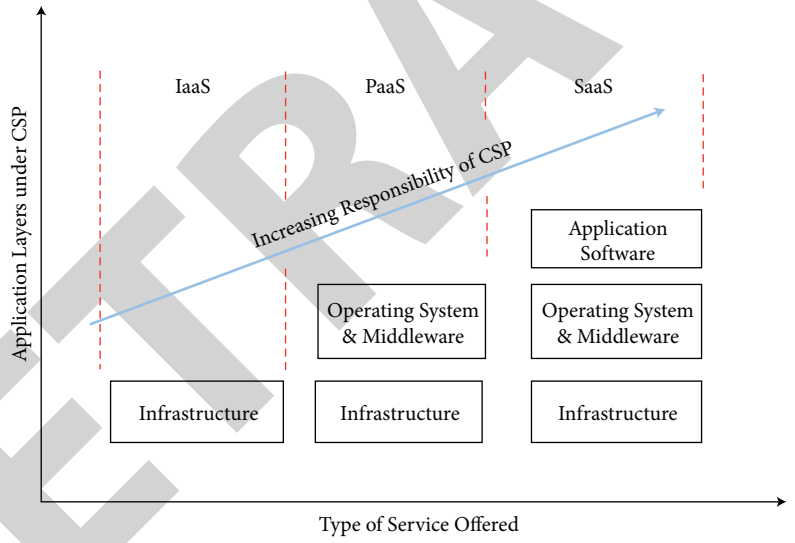

Figure 6: Responsibility of CSPs.

of trust among CC and CSP. Under the prescribed standard, CC can conduct periodic audits of their CSPs to check the veracity of CSP's promised Quality of Service (QoS) as mentioned in the SLAs. As the CC and CSP jointly implement cloud services, it is paramount that both carry out periodic risk management exercises to weed out the potential future vulnerabilities [39].

Due to the interlinkages using the Internet, virtually all the physical devices in some form or the other seek or load information over the network. The horizon of cyberspace has broadened the scope of malware and virus to an extent where the entire network of critical infrastructure (servers or ICT hardware) can be hijacked, jeopardizing nations' national security. For instance, a case-in-point is STUXNET, a computer-based virus that disabled Iran's nuclear in 2010 by attacking the SCADA systems. Some of the recent malicious cyber objects are:

(i) Ransomware: it is a targeted attack on individuals or organizations resulting in denial or limited access to personal information, thereby demanding a ransom to regain access. E.g., WAnnaCry in 2017 affected 230,000 windows computers across 150 countries worldwide by locking access to confidential information in exchange for money [40].

(ii) Distributed Denial of Services (DDoS): it burdens the computer servers by artificially creating virtual traffic using Botnets, thereby purposefully crashing

the servers and leading to a denial of services for genuine users, e.g., Malware Saposhi, Reaper, and Mirai.

(iii) Cryptojacking: the attacker covertly uses the user's devices (computers, tablets, or mobile) to mine cryptocurrency without their consent or knowledge.

(iv) StrandHogg: it was a malware attack on all Android devices wherein a malicious app masquerades as a genuine app, thus tricking the users into entering their sensitive information.

(v) Pegasus: a surveillance spyware allegedly developed by Israel based NSO group. It can be covertly installed on all iOS and Android devices and transmit sensitive information (messages, photos, call details, location, passwords) to the attacker.

The waging cybersecurity challenges have turned cyberspace into cyber warfare in the form of Ransomware, Distributed Denial of Services (DDoS), and spyware (as discussed above) [41]. Most digital devices leverage a cloud-based network to communicate and process the data in real-time. The entire banking network and financial services operate through a centralized cloud-based network, gradually digitalizing every possible hitherto physical process. Without adequate cybersecurity measures, a potential click of a mouse can hold a whole nation to ransom, even leading to bankruptcy. Cloud servers operate based on the concept of the global village. Surprisingly, the world is still in the process of devising local laws to regulate an all-pervasive phenomenon. The time is ripe to set up an international organization (similar to Internet Corporation for Assigned Names and Numbers (ICANN)) that can legislate broad framework law governing the data over the cross-country cloud network. Data breaches or losses should be compensated by fixing monetary liabilities on exchanging parties in the form of Cloud Insurance. This can be achieved by mandating an Escrow Account to ensure customers' data protection in case the CSPs go bankrupt [42].

8. Ways to Address Legal Implications

Let us discuss various instruments already in use to manage legal implications arising from cloud-based data. Until there is no international body, all the legal issues pertaining to cloud data are resolved bilaterally among the involved parties.

(1) Mutual Law Assistance Treaty (MLAT): these are binding treaties signed between two parties (usually countries) to iron out the legal complexities by mutual cooperation. It is a country-specific, customizable legal agreement that addresses the legal issues on a one-to-one basis [43]. MLAT facilitates the dispute resolution mechanism and enables the various stakeholders to arrive at a compromise (shown in Figure 7).

For instance, India has signed MLAT with 39 countries (as of July 2020), and the USA has signed the same with 60 countries. These can prove to be the best instrument for dispute resolution, as the top diplomats, legal experts, or administrators are involved in its formulation, implementation, and periodic review. Even a minute dispute between two private individuals from different geographic jurisdictions can be escalated to the highest level for its resolution. MLAT also helps bypass the costly legal battles fought by an expensive battery of lawyers in the courts.

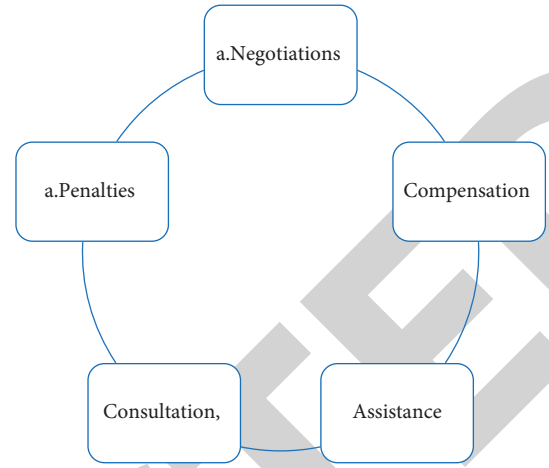

Figure 7: Mechanism used in MLAT.

(2) USA CLOUD (Clarifying the Lawful Overseas Use of Data) Act: the genesis of the act was a dispute between Microsoft and the US govt. This act paved the way for the lawfully retrieving of the data by the US Law Enforcement agencies from technological companies (Google, Apple, etc.), regardless of whether the data is stored in the USA or on foreign land [44]. The basic premise of the act is that companies and individuals have extensive democratic rights while storing, processing, and sharing cloud data. But in case of any reported data breach or criminal activity, USA Law Enforcement agencies have adequate powers to retrieve the data and hold culprits to account. Such a model is the way forward for the countries yet to implement data protection laws or are in the consultative stages of designing data protection laws (like India). Rather than having strict control over the users' data in real-time, let the executive and legal agencies be empowered enough to deal with the contingencies. In some situations, CLOUD [44] conflicts with the European Union's GDPR [26].Under extreme circumstances, the data stored on the cloud services of USA-based companies (such as Amazon Web Services) can be retrieved by USA law enforcement agencies.

Nevertheless, CLOUD Act is the optimal way for the data protection of cloud-based data and serves as a rulebook for the various stakeholders. It is a much-improved way of data protection vis-à-vis the Data Localization obligation under the draft of the Indian Data Protection Bill 2018 [21]. The data localization

Table 1: Summary of existing study.

Domain	Author	Year	Findings
Cybersecurity issues	Campos et al. [41]	2016	Being crucial for the organization, the cloud data needs proper security measures such as encryption, virtual firewalls, ISO standards, etc. While working with Big Data, it is important to have periodic risk management and follow maintenance-oriented lifecycle management using technological solutions. Cyber-insurance should be done with appropriate statistical models to predict associated cybersecurity risks.
	Xu et al. [42]	2019	
Structural issues	Troshani et al. [18]	2011	Cloud computing poses technological, organizational, and jurisdictional risks. The customers are always vulnerable to losing their data permanently or temporarily not able to retrieve data. The CSP and CC should make SLAs as comprehensive as possible and touch upon various untoward scenarios.
	Amron et al. [19]	2019	
Information security risk	Julisch et al. [38]	2010	Information Security Management System (ISMS) under the ISO/IEC 27001 can be extended to cloud computing in the form of Virtual ISMS. The need is the narrow the gap between the CC and CSPs by adhering to adequate standards, audits and keeping the CC informed about the future risks
Jurisdictional risks	Ward et al. [34]	2010	The placement of data servers by CSP at different geographic locations may confront the customer's country's data protection laws/regulations. Further, CSP may also covertly utilize the IaaS, PaaS, or SaaS of their peers across the globe without informing the CC. Jurisdictional issues are the root cause of the exuberant litigation cost incurred by the CSPs. There is an absence of any international organization that provides general framework law in the cloud computing domain.
	Hon et al. [15]	2012	
Power consumption risks	Liu et al. [32]	2020	The mushrooming of data centers across the globe may adversely affect the environment due to massive energy requirements. It is paramount to source the green energy solutions and place the data centers at an optimal geographic location to minimize carbon emissions. High latitude areas of the Pan-Arctic regions are favorable locations to increase the Power Usage Effectiveness (PUE). Big Data is potentially producing astronomical volumes of data per year loaded onto the cloud storage, thereby expanding the energy footprint of cloud devices.
	Perrons. [20]	2015	
Legal issues and territorial disputes	Powell et al. [45]	2010	Peaceful resolution of disputes is essential while settling cross-country cloud computing-related conflicts. The literature shows that bilateral negotiations or treaties (77%) are most preferred among the various dispute resolution instruments. Sometimes federated data regulations (as in the USA) become a bone of contention while dealing with cross-country data protection laws. In many cases, the CSPs are often found not honoring their SLAs in letter and spirit and try to subvert the commitments by taking advantage of data protection laws of third world countries (the state that is not part of the original SLA)
	Coyle et al. [22]	2019	
	Vurukonda et al. [23]	2016	
Data governance issues	Štarchoň et al. [29]	2019	General Data Protection Regulation (GDPR) serves as the gold standard in the international forum in the realm of myriad data protection laws. As cloud computing involves remote storage and data processing, it can be governed by various domestic and international IT (Information Technology) laws and data protection acts. In extreme situations, specific domestic national security laws (e.g., US PATRIOT Act) can lawfully coerce CSPs to divulge their users' data. Such ambiguities require a rule-based approach.
	Goddard. [28]	2017	
	Penasa et al. [27]	2018	
	Al-Ruithe et al. [14]	2017	

provision may be an unnecessary burden for the technology companies and can be impractical. It is the biggest hurdle for Indian Inc and hampers the govt flagship initiative of ease of doing business. Moreover, virtualization is an essential feature of cloud computing, wherein virtual servers, in conjunction with the anonymity feature of the Internet, make it impossible to track the location of the data hosted on different servers across the globe.

(3) Bilateral Treaties: as an instrument for legal assistance, it is quite broad in its objectives, framework, and mandate. Still, it can act as a bridging agreement for addressing the legal issues arising in the field of cloud-based data between two countries. Under such treaties, a unique mechanism can be established in the form of a dedicated formal dispute resolution tribunal/court. The treaty defines the guidelines related to cloud-based data, and the hierarchy of the formal setup can be built on a mutual consensus basis [45].

(4) In-house capability: this is preferred when the govt wants to store confidential data on the cloud. The dependence on the private service provider always has elements of suspicion, especially when storing classified data on cloud-based servers. The govt needs to strengthen the domestic cloud capabilities,

be it private or public, by locating the servers inside the territory of India. This improves the surveillance capabilities of the govt/regulator, and the response time in case of any reported data breach is minimized. For instance, Govt of India (GoI) launched its in-house cloud MeghRaj in 2014 [16]. Such indigenous initiatives help bypass the intrajurisdictional issues arising from the placement of servers in different geographic locations. But due to the widespread accessibility and acceptability of cloud-based services of private players (Google, Apple, Microsoft, etc.) in the public domain, in-house capabilities have minimal scope. Further, the govt is burdened with additional investment and maintenance expenditure for the servers, considering when it has an option of outsourcing cloud services at reasonable rates.

(5) International institution: modelled on the lines, for instance, WHO (World Health Organization), there is an urgent need for an international institution in the field of cloud computing to perform regulatory and arbitration functions. The multiplicity of data governance laws and country-specific legislation governing the ICT domain come at loggerheads resulting in jurisdiction issues. Though the technology has transcended all the conventional approaches, the scope of negotiations in settling international disputes cannot be substituted. The presence of the global institution in ensuring rule-based order, per se, might not be a silver bullet. Still, it will go a long way in adopting standard operating procedures (SoP) across the cloud-computing industry. Today cloud hosts a variety of multisectoral data restrained through domestic data laws. An international institution with the participation of multiple stakeholders (states, policymakers, NGOs, civil societies, and industry) will help in consensus-based decision-making and provide a level playing field to all CSPs irrespective of their financial underpinning.

9. Conclusion

MSMEs have proven to be engines of growth, especially in the context of developing nations. The employment generation potential of the sector can propel economies out of the pandemic-related financial distress. In the 21st century, Cloud computing serves as the bedrock of ICT-enabled service delivery. Post LPG era (Liberalization, Privatization, and Globalization) of 1991, the imports and presence of international players on Indian soil took precedence over indigenous manufacturing and production. This led to the dismal contribution of MSMEs in the total output or worse, even the closure of some successful firms outwitted by the technological prowess of international behemoths. Time and again, certain natural (COVID-19) and artificial (Russia-Ukraine war) catastrophes have shown the significance of the self-reliability of means of production. MSMEs empowerment has again resurfaced among the policymakers; thereby, the government is ready to do handholding, as and when required. Technological advancement of MSMEs remedied myriad structural (cost saving, just-in-time approach, etc.) and functional (global presence, moving up the value chain, etc.) issues. Today's solution can become tomorrow's problem; the same seems to work in the realm of cloud computing. MSMEs are not equipped to defend astronomical litigation expenses due to their slim operating margins. Further, the international lawsuits are also time-consuming and may take several years for consensual resettlement. Hence, the international multilateral organizations and the national governments need to devise mechanisms and procedures to deter cloud-related legal challenges.

The era of cloud computing has just begun, and the time is not far when the use of physical memory devices will become obsolete. In the Indian context, the Right to Privacy is a fundamental right that protects cloud-based data from possible data breaches and thefts. There is an urgent need to establish an international body/commission for the Global Governance of cloud data and adherence to a rule-based order. It will assist in generating vertical accountability and streamline the legal issues arising in the realm of cloud computing. We also need robust legislative support from the government in the form of a Data Protection law. The suggestion of Data Localization needs reconsideration, and mechanisms are required to empower the law enforcement agencies with adequate provisions to bring cybercriminals to book. By its very definition, the Internet is anonymous and pervasive; therefore, laws that prescribe parochialism and localization of data need to be eschewed. The spirit of More Governance and Less Govt is the key to addressing the legal issues. The benchmark of good governance is forming a society where the freedom of individuals is equally respected, and restrictions are imposed only when necessary. Another area of concern is to lower the legal cost of compliance. The Indian courts are already burdened with a backlog of 3.5 crore cases. Urgent steps need to be taken to encourage out-of-court settlement in the form of consultation, consensus, and negotiation with the disputed parties. The laws must be formulated to provide more clarity and address the grey areas. Cloud computing is the necessity of every department, ministry, and sector; hence the laws need to be broad-based, providing flexibility to the executives. During the legislative process of cloud-based data, the respective departments should be given space to voice their recommendation to cover technical and micro details. Interdepartmental consultation is required before designing the final draft of the Data Protection law. The Industrial Revolution 4.0 is the future, including cyber-physical systems, automation, and cloud computing is at the core of it. Table 1 shows the study of all the existing work from the field of legal issues in cloud computing.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

Jaskaran Singh Saini, Dinesh Kumar Saini, and Punit Gupta designed the objective of the work and the issues to be discussed in this work in the field of cloud computing.

Chhattar Singh Lamba and G Madhusudhana Rao has contributed in the legal issues section and international issues in the field of cloud computing. It is a contribution of each author and all authors discussed the work and contributed to the final manuscript. All authors confirm sole responsibility for the following: study conception, data collection, analysis and manuscript preparation.

References

[1] Markets and Markets, "Cloud clomputing market size, share and global market forecast to 2026 | covid-19 impact analysis," 2021, https://www.marketsandmarkets.com/Market-Reports/cloud-computing-market-234.html.

[2] K. Eric, "What cloud computing really means | InfoWorld," 2016, http://www.infoworld.com/article/2683784/cloud-computing/what-cloud-computing-really-means.html.

[3] W. Kim, "Cloud computing: today and tomorrow," *Journal of Object Technology*, vol. 8, no. 1, p. 65, 2009.

[4] S and M E Ministry of micro, "Annual Report 2021-22," 2021, http://www.msme.gov.in.

[5] India Brand Equity Foundation, "MSME sector - imperative to lift Indian economy | IBEF," 2022, https://www.ibef.org/blogs/msme-sector-imperative-to-lift-indian-economy.

[6] A. Vanessa Ratten, "Social entrepreneurship through digital communication in farming," *World Journal of Entrepreneurship, Management and Sustainable Development*, vol. 34, no. 1, pp. 1–5, 2018.

[7] Cable co uk, "Worldwide mobile data pricing 2021 | 1GB cost in 230 countries," 2021, https://www.cable.co.uk/mobiles/worldwide-data-pricing/.

[8] R. D. Raut, B. B. Gardas, M. K. Jha, and P. Priyadarshinee, "Examining the critical success factors of cloud computing adoption in the MSMEs by using ISM model," *The Journal of High Technology Management Research*, vol. 28, no. 2, pp. 125–141, 2017.

[9] P. Gupta, A. Seetharaman, and J. R. Raj, "The usage and adoption of cloud computing by small and medium businesses," *International Journal of Information Management*, vol. 33, no. 5, pp. 861–874, 2013.

[10] Ministry of Finance, "Economic survey 2015-16," 2015, https://www.indiabudget.gov.in/budget2016-2017/es2015-16/echapter-vol1.pdf.

[11] Ministry of Finance, "Budget 2022-23," 2022, https://www.indiabudget.gov.in/.

[12] W. H. Liao, P. W. Chen, and S. C. Kuai, "A resource provision strategy for software-as-a-service in cloud computing," *Procedia Computer Science*, vol. 110, pp. 94–101, 2017.

[13] L. Deng, Z. Yang, P. Du, and Y. Song, "A cloud platform for space science mission concurrent design," *Concurrent Engineering*, vol. 26, no. 1, pp. 104–116, 2018.

[14] M. Al-Ruithe and E. Benkhelifa, "Analysis and classification of barriers and critical success factors for implementing a cloud data governance strategy," *Procedia Computer Science*, vol. 113, pp. 223–232, 2017.

[15] W. K. Hon, J. Hörnle, and C. Millard, "Data protection jurisdiction and cloud computing - when are cloud users and providers subject to EU data protection law? The cloud of unknowing," *International Review of Law, Computers & Technology*, vol. 26, no. 2-3, pp. 129–164, 2012.

[16] Department of Electronics and Information Technology, "Government of India ' s Gi Cloud (Meghraj) Strategic direction paper," 2013, https://www.meity.gov.in/writereaddata/files/GI-Cloud%20Strategic%20Direction%20Report%281%29_0.pdf.

[17] S. I. Tay, T. C. Lee, N. Z. A. Hamid, and A. N. A. Ahmad, "An overview of industry 4.0: definition, components, and government initiatives," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 10, no. 14, pp. 1379–1387, 2018.

[18] I. Troshani, G. Rampersad, and N. Wickramasinghe, "On cloud nine? An integrative risk management framework for cloud computing," in *Proceedings of the 24th Bled e Conference eFuture: Creating Solution for the individual Organisations and Society*, Bled, Slovenia, June 2011.

[19] M. T. Amron, R. Ibrahim, N. A. A. Bakar, and S. Chuprat, "Acceptance of cloud computing in the Malaysian public sector: a proposed model," *International Journal of Engineering Business Management*, vol. 11, Article ID 184797901988070, 2019.

[20] R. K. Perrons, "How the Energy Sector Could Get it Wrong with Cloud Computing," *Energy Exploration & Exploitation*, vol. 33, 2015.

[21] Ministry of Electronics and Information Technology, "Personal Data Protection Bill 2018," *The Gazette of India*, vol. 1, pp. 1–25, 2018.

[22] D. Coyle and D. Nguyen, "Cloud computing, cross-border data flows and new challenges for measurement in economics," *National Institute Economic Review*, vol. 249, 2019.

[23] N. Vurukonda and B. T. Rao, "A study on data storage security issues in cloud computing," *Procedia Computer Science*, vol. 92, pp. 128–135, 2016.

[24] R. T. Sataloff, M. M. Johns, and K. M. Kost, "Agreement on trade-related aspects of intellectual property rights," pp. 319–351, 1994, https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm.

[25] A. Gurumurthy and N. Chami, "Governing the resource of data: to what end and for whom? Conceptual building blocks of a semi-commons approach," 2022, https://datagovernance.org/report/governing-the-resource-of-data-to-what-end-and-for-whom-conceptual-building-blocks-of-a-semi-commons-approach.

[26] European Parliament and of the Council, "Regulation (eu) 2016/679 of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation)," *Official Journal of the European Communities*, vol. OJ L 119/1, pp. 1–88, 2016, http://data.europa.eu/eli/reg/2016/679/oj.

[27] I. Penasa, C. de Miguel Beriain, A. Barbosa et al., "The EU general data protection regulation: how will it impact the regulation of research biobanks? Setting the legal frame in the Mediterranean and Eastern European area," *Medical Law International*, vol. 18, no. 4, pp. 241–255, Dec. 2018.

[28] M. Goddard, "The EU general data protection regulation (GDPR): European regulation that has a global impact," *International Journal of Market Research*, vol. 59, no. 6, pp. 703–705, 2017.

[29] P. Štarchoň and T. Pikulík, "GDPR principles in data protection encourage pseudonymization through most popular and full-personalized devices - mobile phones," *Procedia Computer Science*, vol. 151, pp. 303–312, 2019.

[30] A. Bharat Abhiyan, "Atmanirbhar Bharat abhiyan," *Press Information Bureau*, vol. 1, no. 1, pp. 1–27, 2020.

[31] I. Bird, "Computing for the Large Hadron collider," *Annual Review of Nuclear and Particle Science*, vol. 61, no. 1, pp. 99–118, 2011.

[32] Y. Liu, X. Wei, J. Xiao, Z. Liu, Y. Xu, and Y. Tian, "Energy consumption and emission mitigation prediction based on data center traffic and PUE for global data centers," *Global Energy Interconnection*, vol. 3, no. 3, pp. 272–282, Jun. 2020.
[33] R. Buyya, C. Vecchiola, and S. T. Selvi, "Advanced topics in cloud computing," in *Mastering Cloud Computing*, pp. 373–427, Elsevier, Amsterdam, Netherlands, 2013.
[34] B. T. Ward and J. C. Sipior, "The internet jurisdiction risk of cloud computing," *Information Systems Management*, vol. 27, no. 4, pp. 334–339, 2010.
[35] USA PATRIOT Act, "uniting and strengthening america by providing appropriate tools required to intercept and obstruct terrorism (usa patriot act) act of 2001," 2001, https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act.
[36] Data Protection Working Party, "Article 29 data protection working party update of opinion on applicable law 1 in light of the cjeu judgement in google spain 2," 010, http://ec.europa.eu/justice/data-protection/index_en.htm.
[37] Iso/Iec 27001:2013, "ISO - ISO/IEC 27001:2013 - information technology — security techniques — information security management systems — Requirements," 2022, https://www.iso.org/standard/54534.html.
[38] K. Julisch and M. Hall, "Security and control in the cloud," *Information Security Journal: A Global Perspective*, vol. 19, no. 6, pp. 299–309, 2010.
[39] D. Catteddu and G. Hogben, "Benefits, Risks and Recommendations for Information Security," in *Proceedings of the Iberic Web Application Security Conference 2009*, Madrid, Spain, December 2009.
[40] Bbc, "WannaCry ransomware attack," 2017, https://www.bbc.com/news/technology-41753022.
[41] J. Campos, P. Sharma, E. Jantunen, D. Baglee, and L. Fumagalli, "The challenges of cybersecurity frameworks to protect data required for the development of advanced maintenance," *Procedia CIRP*, vol. 47, pp. 222–227, 2016.
[42] M. Xu and L. Hua, "Cybersecurity insurance: modeling and pricing," *North American Actuarial Journal*, vol. 23, no. 2, pp. 220–249, 2019.
[43] Goverment of The United States of America, "Treaty between the government of the republic of india and the government of the united states of america on mutual legal assistance in criminal matters," 2001, https://www.mea.gov.in/TreatyDetail.htm?890.
[44] Senate of the United States, "Clarifying lawful Overseas use of data act or the 'CLOUD act," vol. 1, pp. 1–32, 2018, https://www.hatch.senate.gov/public/_cache/files/6ba62ebd-52ca-4cf8-9bd0-818a953448f7/ALB18102 (1).pdf.
[45] E. J. Powell and K. E. Wiegand, "Legal systems and peaceful attempts to resolve territorial disputes," *Conflict Management and Peace Science*, vol. 27, no. 2, pp. 129–151, 2010.