ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 10, October 2013

A Cross Border Access to Data Stored In the Cloud

K.Senathipathi[1], Dr.S.Chitra[2], J.Angeline Rubella, M.Suganya[3]
1. Assistant Professor, VSB College of Engineering, Coimbatore.
2. Principal, Er.Perumal Manimegalai Engineering College, Hosur.
3. Assistant Professors, KPR Institute of Engineering and Technology, Coimbatore.

Abstract:

Providers of cloud computing services are increasingly serving customers outside their home markets and using service delivery models that require the transmission of data across borders. The article explores the role of cloud computing in cross border. The main policy challenges associated with cross-border cloud computing are data privacy, security, and ensuring the free flow of information is explored. Finally, the particular challenges faced by developing countries as they seek to participate in the market for cloud computing services. This review include case study of one of the most important emerging markets for such services—India.

Index Terms – Cross border, Data privacy, Security, challenge.

Introduction

This paper examines the extent to which access to data in the Cloud by governments in various jurisdictions is possible, regardless of where a Cloud provider is located. "Governmental access," as that term is used here, includes access by all types of law enforcement authorities and other governmental agencies, recognizing that the rules may be different for law enforcement and national security access. Governments need some degree of access to data for criminal (including cyber crime) investigations and for purposes of national security. But privacy and confidentiality also are important issues. As cloud technology evolves, policies in the areas of data privacy, security, and the free flow of data struggle to keep pace. Policymakers use various tools, including international cooperative forums, bilateral and multilateral trade agreements, and domestic policy to address challenges in these areas. Meanwhile, developing countries such as China and India seek to participate in this growing industry and need to consider both international policy uncertainties related to the cloud as well as their own domestic infrastructure and regulatory challenges for effective contribution to the development of the industry. We provide brief study of what India is doing to meet these challenges.

1. Role of Cloud Computing In Cross-Border

Developing countries such as China and India seek to participate in this growing industry and need to consider both international policy uncertainties related to the cloud as well as their own domestic infrastructure and regulatory challenges through effective contribution for the development of the industry. Hence a brief study was made on the efforts taken by the countries to meet these challenges.

In addition to domestic legal frameworks enabling governmental access to data within a country, Mutual Legal Assistance Treaties ("MLATs"), which are in effect between and among countries around the world, can provide governments the ability to access data stored in one jurisdiction but needed for lawful investigative purposes in another. Despite the procedural hurdles that may exist to request and obtain information pursuant to MLATs, these treaties make borders and the physical location of data much less significant barriers to governmental access. The existence of MLATs diminishes any argument that data stored in one jurisdiction is immune

from access by governmental authorities in another jurisdiction. For example, Germany signed a Mutual Legal Assistance Treaty in Criminal Matters with the United States in 2003 and a Supplementary Treaty to the Mutual Legal Assistance Treaty in Criminal Matters in 2006. Both treaties entered into force on October 18, 2009 and allow authorities in each country to request and receive information located in the other's jurisdiction (including information stored in third-party facilities).

On a related issue, there is significant discussion today about the power of a government to require a party in its jurisdiction to access and produce data stored in another jurisdiction, based on principles of physical presence of the party (not the data, or where the party is headquartered). In other words, the fact that a business located in one country may have chosen to store its data in the Cloud in another country does not mean that the business is immune from governmental demands for the production of that off-shored data. Of the countries we surveyed, Germany and Japan are the only two that, in some instances, limit the data that the government can access to that which is physically located on servers within their national borders.

There is the real potential of data relating to a person, but not technically "personal data," stored in the Cloud being disclosed to governmental authorities voluntarily, without legal process and protections. In other words, governmental authorities can use their "influence" with Cloud service providers – who, it can be assumed, will be incentivized to cooperate since it is a governmental authority asking – to hand over information outside of any legal framework.

It is concluded that civil rights and privacy protections related to governmental access to data in the Cloud are not significantly stronger or weaker in any one jurisdiction, and that any perceived locational advantage of stored Cloud data can be rendered irrelevant by MLATs. Our review reveals that businesses mislead themselves and their customers if they rely on an assumption that selecting Cloud service providers based in one jurisdiction or another better insulates data from governmental access. Instead, this study indicates that it is on business' interest to support governmental cooperation in this area, as it is the consistent and reasonably restrained exercise of existing legal authorities that will enable the economic growth and other benefits of Cloud computing.

1.1 Methodology

The experienced local counsels were consulted about data protection and governmental access law in each of the jurisdictions and asking the following questions for each jurisdiction:

1. May government require a Cloud provider to disclose customer data in the course of a government investigation?
2. May a Cloud provider voluntarily disclose customer data to the government in response to an informal request?
3. If a Cloud provider must disclose customer data to the government, must the Cloud provider notify the customer?
4. May government monitor electronic communications sent through the systems of a Cloud provider?
5. Are government orders to disclose customer data subject to review by a judge?

6. If a Cloud provider stores data on servers in another country, can the government require the Cloud provider to access and disclose it?

MLATs effectively make a country's borders less significant for purposes of governmental access to data, and likewise make less significant the location of a Cloud service provider within one country's borders as opposed to another country's borders

1.2 Mutual Legal Assistance Treaties

Governmental authorities are able to reach data stored on the servers of a Cloud service provider over whom they do not have jurisdiction through an MLAT with a foreign nation where the Cloud service provider is based. For example, the United States and member states in the European Union have entered into bilateral MLATs that allow governmental authorities on both sides of the Atlantic to request access to data stored on the servers of a Cloud service provider physically located in or subject to the jurisdiction of the foreign nation.

2. Privacy and Security of Cloud in Cross Border

The review was turned to the principal issues that policymakers face with respect to cross-border provision of cloud computing services. Hence the following three topics have been focused: data privacy, security, and restrictions on where data are housed One area of policy that heavily affects the provision of cloud services is data privacy. Countries' domestic data privacy laws can vary quite substantially and often affect foreign companies seeking to provide any type of electronic service to consumers in that country.

2.1 Data Privacy

Among the major markets that have adopted some form of comprehensive data privacy law are India, Japan, Malaysia, South Korea, and Taiwan. China, Singapore, and Thailand are among the countries that, like the U.S., have not adopted comprehensive, mandatory regulations.

The differences in data privacy laws are of major significance for cloud computing providers seeking to serve customers in multiple countries. Cloud computing providers may need to collect personal data from customers in order to serve them. For example, a cloud-based travel booking site for employees may store personal information about the users, such as their full names and addresses. Providers may also store or process personal data relating to their customers' customers. For example, a cloud-based customer relationship management database is likely to contain contact information or other personal details about the client firm's customers. Cloud providers must ensure that data storage and processing complies with laws in all relevant jurisdictions, and this can become even more complicated when data are stored and processed globally, not just in the cloud provider's home country or the customer's home country.

In some cases, this complexity may limit a provider's ability to do business in multiple markets. Recognizing the differences in domestic data privacy regimes, there have been a number of international efforts through multilateral organizations to develop a common framework for cloud-related policy. The two most notable of these are the efforts of the Organization for Economic Cooperation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC)

forum. Both organizations have focused primarily on developing a shared set of principles for data privacy.

The Guidelines establish several rights of the individual pertaining to his or her personal data and lay out framework principles that national governments should follow in protecting these rights. Of most relevance for international trade in cloud services are paragraphs 15–18 outlining these principles, which read as follows:

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

The Guidelines also encourage countries to support industry self-regulation where possible. Overall, while the Guidelines established some principles that have guided the direction of countries' data privacy laws, they also preserve a great deal of flexibility, as evidenced by the very different data privacy regimes among OECD countries. From the perspective of one cloud policy expert, the main contribution of the OECD Guidelines is that they seek to "keep governments out of the way" in most cases.

The core principle in the APEC Framework is "accountability" it means, the entity that collects personal information and is responsible for ensuring which was handled in accordance with the privacy guidelines in the Framework (as implemented by the participating country), regardless of where that information travels. While cloud industry officials generally feel the APEC Framework was a good step, more than one mentioned that the implementation remains in flux. One commented that he found APEC's approach potentially very useful and views it as a counterbalance to the European approach.

2.2 Security

The concept of security in the context of cloud computing generally refers to ensuring that unauthorized parties do not obtain access to sensitive data. In that sense, security is related to privacy. Indeed, certain domestic laws that obligate service providers to protect data in certain sectors, such as the Gramm-Leach-Bliley Act for financial services and HIPAA for healthcare providers can be considered both privacy and security measures.

Outside of specially protected sectors, it is usually up to the parties to include a security framework in the contract for cloud computing services. Some organizations have valid concerns about entrusting the security of their data to a third party, especially when the information being stored with the cloud provider is proprietary or sensitive. Cloud providers, however, argue that the cloud actually offers some security advantages. Because services are centralized and resources are pooled in the cloud model, providers may be able to better predict and detect threats to the network. In the event that a security breach occurs, a cloud provider may be able to more quickly eliminate the threat since the solution does not need to be applied to multiple end users' machines. Large cloud providers are also able to recruit top computer security talent.

Cloud providers operating in international markets are concerned that an interest in ensuring security can sometimes lead to "knee-jerk reactions" by governments. Especially when there is a major security breach, governments are more likely to pursue tighter regulation, which may inhibit the development of the market. For example, in the wake of the Mumbai terrorist attacks, the Indian government invoked national security to require access to all BlackBerry communications in India. In terms of international cooperation on data security policy, a set of OECD Guidelines offers basic principles. These Guidelines for the Security of Information Networks and Systems (last updated in 2002) are broad and provide suggestions for how participants in information systems and networks can better anticipate risks, design and adapt security policies, and respond to threats, while preserving the rights of individuals. There are also international standards, developed by the International Standards Organization and the International Electro technical Commission that provide guidance on how best to manage information security and allow organizations to seek certification of their information security controls.

Cloud providers have expressed concerns about "localization requirements" that compel firms storing and processing data for clients from a given country to locate the data in that country. Governments typically create such requirements for the ostensible purpose of keeping data private and secure. Localization requirements are problematic for cloud providers, as "location independence" is a core aspect of the cloud delivery model. Policies that require providers to locate facilities in a given location may leave them with the choice of selecting a sub-optimal location or not serving the targeted market at all.

Governments may also restrict the locations at which official government data may be housed and processed. Although such requirements may sometimes be necessary to restrict access to sensitive or classified data, some government data may be sufficiently non-sensitive to make storage on foreign servers acceptable.

3. Challenges Faced By Developing Countries - India

Developed countries account for most of the supply and consumption of cloud computing services, and have been at the forefront of international policymaking on cross-border data flows. Yet governments and private parties in many developing countries are

eager to expand those countries' role as suppliers and consumers of cloud computing services. They see cloud computing and other IT service industries as potential sources of high-paying jobs and drivers of economic growth—both directly, through the success of firms providing IT services, and indirectly, via the "spillover" benefits to other industries of increased access to advanced technology. Some countries may also hope to reduce dependence on Foreign Service providers for strategic reasons.

A variety of factors determine whether a country has a propitious environment for supply and consumption of cloud computing services. The Asia Cloud Computing Association (ACCA) published a list of ten such factors for its "Cloud Readiness Index.". They include:

• regulatory conditions (including intellectual property protection)

•international connectivity (including price and availability of bandwidth for international connections)

•quality of data protection policies

•broadband quality (including penetration levels as well as reliability of connections)

•power grid quality

•pervasiveness of Internet filtering

•"business efficiency" (including a variety of conditions that affect the ease of doing business, such as labor costs, productivity, financial market development, and the quality of corporate governance)

• risk (including macroeconomic, security, social, and environmental factors) level of development of information and communication technologies (ICTs)

• level of government support for development of ICTs, and cloud computing specifically.

While the ACCA gives each of these factors equal weight, one might argue that the factors vary in importance according to the cloud service in question. For example, labor costs and workforce skills are less important for data center operations, because each center requires only a few workers. On the other hand, skilled software developers are critical for the development of PaaS and SaaS. Cheap electricity and the cost and reliability of water supply are especially important for ensuring that large data centers—one of the key building blocks for IaaS—are properly cooled. Internet filtering is particularly problematic for SaaS, as censors may hinder or block entirely the public's use of specific applications, but filtering may also cause broader connectivity problems (e.g., slower data transfers) that affect the full range of cloud services. There may also be factors not included in the index that are important. One example is the cost of land, which may affect providers' decisions on where to locate data centers in light of their massive size.

Many developing countries have made less progress than wealthier countries in creating and enforcing legal frameworks important for cloud computing (e.g., for data privacy and protection and intellectual property rights), and the quality of water, power, and broadband infrastructure in such countries often lags that in richer countries.

INDIA

India's rise to prominence in the global computer services industry is

among the country's great economic success stories. India is the world's leading exporter of computer and information services, with exports totaling $33.8 billion in 2009.

Indian firms such as TCS, Wipro, and Infosys are among the most important in the industry worldwide. India's computer services industry has succeeded due to a liberal policy toward foreign investment in the industry; government support for the industry's development through programs such as the Software Technology Parks of India (STPI), which granted eligible firms benefits such as lower taxes and duty-free imports and a supply of skilled, English-speaking workers willing to work for wages lower (albeit rising) than those paid to similar workers in developed countries.

Cloud computing is a potential threat to India's computer services industry. One of the principal offerings of India's largest computer services firms is information technology outsourcing, in which the provider fulfills a broad range of information technology services for the client, such as management of data centers and processing of data (on-site or remotely). IaaS is sometimes viewed as a replacement for elements of traditional IT outsourcing—and thus, a potential threat to the present industry leaders. One recent survey of corporate decision-makers lends credence to this view: 47 percent of respondents said cloud specialist companies (such as Rackspace and Amazon Web Services) were best suited to manage private clouds, compared to 39 percent who said that traditional IT outsourcers were best.

At the same time, numerous information technology firms in India are moving aggressively into cloud services, across all three service models (SaaS, PaaS, and IaaS). Some are "pure play" cloud specialists—cloud services are their core, or only, offerings.

Demand for cloud computing services in India is growing along with supply. One consulting firm estimated the size of the Indian market for public cloud services at $88 million in 2010, and the private cloud market as three-and-a-half times larger. The same source estimated that the share of India's IT spending devoted to cloud services would increase from 1.4 percent in 2010 to 8.2 percent in 2015.

The Indian firms have had notable successes in supplying and adopting cloud computing, there are factors that pose long-term challenges to India's competitiveness in cloud services provision, and IT services more broadly. One is the challenge of securing affordable and reliable sources of energy. The data centers which store and process data for cloud activities use great amounts of energy, but electricity is expensive, scarce, and unreliable. While firms have often relied on private sources of power, such as generators, to ensure that their needs are met, the growth of data centers could ultimately be constrained by the weak electricity infrastructure.

Rules promulgated in 2011 were intended to clarify the meaning of "reasonable security practices" and the circumstances under which parties can be held liable for damages, but only led to further confusion. Notably, the extent to which the rules apply to data associated with individuals outside India (and thus, to cross-border data flows) was not made clear. The implications of this ambiguity for trade could be significant. For example, Indian providers of data storage and processing

services might demand that their clients adjust their internal data protection procedures, for fear of unwittingly falling afoul of section 43A. The full implications of this provision on cross-border data flows will depend on additional government guidance.

CONCLUSION:

Estimates of the size of the global market for cloud computing services vary, but few observers doubt that it is a multi-billion dollar industry growing rapidly. Provision of cloud services across borders is already substantial, and is likely to grow along with the broader market for such services.

Governments have sought to address the chief policy challenges associated with trade in cloud services—ensuring data privacy, security, and the free flow of data—through domestic policies, bilateral agreements, and multilateral institutions. On the international level, approaches have included establishing non-mandatory, best-practice guidelines as well as binding commitments.

Developing countries have played a smaller role than developed countries in the market of cloud services and international policymaking related to the cloud. Many developing countries are lack on the domestic policies and infrastructure needed to develop more on their cloud industries, but governments and private parties in some of these countries are seeking to address these gaps. China and India illustrate the great potential for growth of cloud computing as well as the scope and variety of the challenges to overcome.

REFERENCES:

[1] Renee Berry and Matthew Reisman, Policy Challenges of Cross-Border Cloud Computing" , United states International Trade Commission journal of International commerce and Economics" , web version, 2012.

[2} Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li ,"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, Vol. 22, No. 5, 2011.

[3] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Privacy Preserving Public Auditing for Data Storage Security in cloud Computing", 2010.

[4] Ramgovind S, Eloff MM, Smith E ,"The Management of Security in Cloud omputing", School of Computing, University of South Africa, Pretoria, South Africa ©2010

[5] Jianfeng Yang and Zhibin Chen ," Cloud Computing Research and Security Issues", IEEE 2010.

[6] S. Sajithabanu and Dr. E. George prakash Raj, "Data Storage Security in Cloud" IJCST Vol. 2, Issue 4, Oct.-Dec. 2011.

[7] Sunita Rani and Ambrish Gangal, "Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints", (IJCSIT) ,Vol. 3 (3) , 2012,4302 –4304.

[8] Alok Tripath and Abhinav Mishra," Cloud Computing Security Considerations", IT Division, DOEACC Society, Gorakhpur Centre Gorakhpur, India, 2010, IEEE.

[9] "Advance Computer Technology" a book by Dr. Deven shah. Edition -2011.

[10] Rupali Sachin Vairagade and Nitin Ashokrao Vairagade " Cloud computing data storage and security enhancement" (IJARCET) Volume 1, Issue 6 August 2012, 145-149.