IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

World Wide Web - Cloud Boundaries

Saroj Kumar[1*], Santosh Kumar[2]

[1,2] Dept. of Computer Science and Engineering, Maharishi University of Information Technology, Lucknow, India

Corresponding Author: saroj.kumar999@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i6.483490 | Available online at: www.ijcseonline.org

Accepted: 12/Jun/2019, Published: 30/Jun/2019

***Abstract*—** In the present post-industrial information epoch where the regular changing environment is depend upon technological abbreviations. Early world was related information with only joining two computers to each other, upto this secure cloud computing policies. Present world races are in racing mode where everyone want to become a leader. Today's world war is based on information. Information is based on privacy concern over Assess, Compliance, Storage, Monitoring and privacy breaches. Over this phenomena world decide many rules and regulations as per their feasibility to provide information over cloud that still world is in need of better policies over geographical boundaries and country based political issues. Many major rules and regulation are define in this paper to maintain worldwide cloud boundaries for use of fast safe and secure.

***Keywords*—** *Cloud, Rapid Adoption of cloud, Barriers to cloud, Legal and Political Issues[40].*

I. INTRODUCTION

It is not important to understand what cloud computing is, but it is more important to understand how this model of computing has evolved. Civilization has progressed in waves (three of them to date: the first wave was agricultural civilization, the second was the industrial era, and the third is the information era). Within each wave, there have been many important sub waves. In this post-industrial information age, we are now at the start of what many people feel will be an era of cloud computing, Information evolution very similar to an important change within the industrial era. Specifically, equates the rise of cloud computing in the information era to electrification in the industrial age. It used to be that organizations had to serve their own power (water wheels, windmills).With electrification, after all, organizations no longer equip their own power; they just plug in to the electrical grid. That cloud computing is really the beginning of the same change for information technology. Right Now organizations provide their own computing resources (power). The emerging future, however, is one in which organizations will simply plug in to the cloud (computing grid) for the computing resources they need. But in cloud computing is not all about services but it also depend on security and privacy. And although all focuses specifically on the economic benefits of cloud computing, but does not discuss information security problems associated with. This paper do, that is the purpose to articulate security and privacy issues associated with to cloud computing [1].

II. HISTORY OF INTERNET

- 1957: U.S. forms Advanced Research Project Agency (ARPA). USSR launched Sputnik, the first artificial Earth satellite. The successive year, the US formed the Advanced Research Projects Agency (ARPA) within the Department of Defense (DoD) to establish US leadership in science and technology applicable to the military.
- 1960s: ARPANET, the forerunner of today's Internet, is formed ARPA wanted to create a computer network that would continue to function in the incident of a disaster, such as a nuclear war, so that if unit of the network was damaged or destroyed the rest of the system would perform. That network was called ARPANET, (Advanced Research Projects Agency Network), which ties US scientific and academic researchers. It was the originator of today's Internet. In time, ARPANET computers were put at every university in the US that had defense associated funding. Gradually, the Internet had gone from a military pipeline to a communications tool for scientists.
- 1970: ARPANET makes its prime cross country connection. The first cross-country link installed by AT&T was between University of California, Los Angeles (UCLA) and Bolt Beranek and Newman, Inc. (BBN).
- 1973: ARPANET makes its prime international connection. The first ARPANET connection exterior to the US was established to NORSAR in Norway in 1973, just before the connection to University College of

London (England). ARPANET had 2000 users at this point, 75% which used it for email.

- 1974: The Internet is born. The term "Internet" was coined by Vinton Cerf, Yogen Dalal and Carl Sunshine at Stanford University to describe a global transmission control protocol/internet protocol (TCP/IP) network, or the rules that let on for information to be sent back and forth over the Internet.
- 1976: Apple Computer is established by Steve Jobs and Steve Wozniak. Prior to Apple, computers were sold in kits that needed assembling. In 1977 Apple Computers introduced the Apple II, the world's premier personal computer, which was huge-marketed and pre-assembled allowing a wider range of people to use computers, concentrated more on software applications and less on the development of the computer.
- 1979: CompuServe became develop the first online service provider to offer e-mail capabilities and technical support to personal computer users. CompuServe was eventually purchased in 1998 by AOL Company, who arrived on the arena in the early 90's. AOL came out with a destructive marketing strategy, new social appearance such as chat rooms and online games, and an updated monthly vs. hourly pricing standard which made the web much more affordable. Millions of brand-new users signed up almost overnight making the web more mainstream.
- 1981: IBM announces its pioneer Personal Computer (PC) A team known as "Project Chess" made the IBM PC, which launched on August 12, 1981. Although not at all cheap, at a base price of US$1,565 it was affordable for businesses and many businesses purchased PCs.
- 1989: ARPANET ends. Sir Tim Berners-Lee creates the World Wide Web, what we have as today's modern Internet. The World Wide Web, or "the Web," although commonly confused with the Internet, is in fact an application built on top of the Internet that connects hypertext pages or web pages. With a Web browser, one can look Web pages that may embedded text, images, videos, and other multimedia and navigate between them having hyperlinks. The World Wide Web enabled the spread of information over the Internet through an easy-to-use and flexible shape. It thus played an important role in popularizing use of the Internet.
- 1993: Mosaic, the first web browser, is formed. Mosaic is the web browser credited with popularizing the World Wide Web. It was created at the National Center for Supercomputing Applications (NCSA) and was one of the first to provide a multimedia graphical user interface that allowed users to more easily navigate the web by converting text commands to images. Mosaic was finally renamed Netscape Navigator, and the company took the 'Netscape' name on November 14, 1994.
- 1996: beginning of browser wars with Netscape and Microsoft leading the charge. Netscape Navigator was the dominant and most widely used web browser at that time, while Microsoft had just released the first version of Internet Explorer as part of the Microsoft Windows 95 plus Pack. Over the next three years the two would introduce new appearance and battle it out for the most users. Netscape was defeated by the end of 1998, after which the company was capture by America Online. Internet Explorer became the new leading browser, attaining a peak of about 96% of the web browser usage share during 2002, more than Netscape had at its crest.
- 1997: Broadband Internet is introduced. High-speed home networking was first introduced in 1997 with a cable modem. DSL (Digital Subscriber Line) was introduced two years later. By 2001 cable and DSL support had quickly surpassed that of dial-up, as the faster speeds allowed users to exploit the newest web applications that were beginning to take shape.
- 1998: Search giant Google is founded. Google began as a research project of Larry Page and Sergey Brin while studying for their Ph.Ds at Stanford University. something that the most relevant page associated with a search were the ones with the most links to them from other highly relevant web pages, Page and Brin tested their thesis as part of their course work and laid the foundation for their search engine, which today is the largest visited site on the web and has become the most powerful brand in the world [2].
- Services on internet called cloud computing.

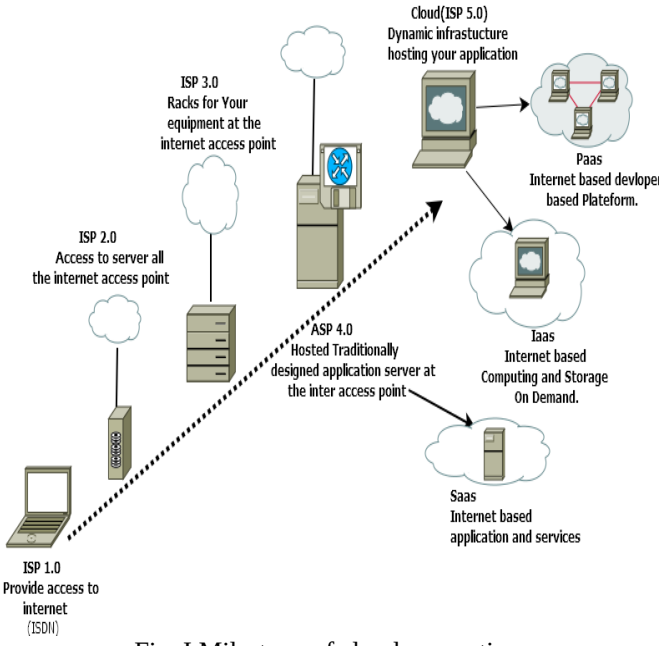

Fig. I Milestone of cloud computing.

III. RAPID ADOPTION OF CLOUD COMPUTING IN ENTERPRISES

Cloud computing is the way future that's why many of enterprises are adopting it. The reason behind that is the benefit of the cloud over the network. Such advantage. As follows.

1. Development and testing.
2. Scalability.
3. Agility.
4. Resource pooling.
5. Cost cutting.
6. One time big data,
7. Cloud based anti spam and antivirus services.

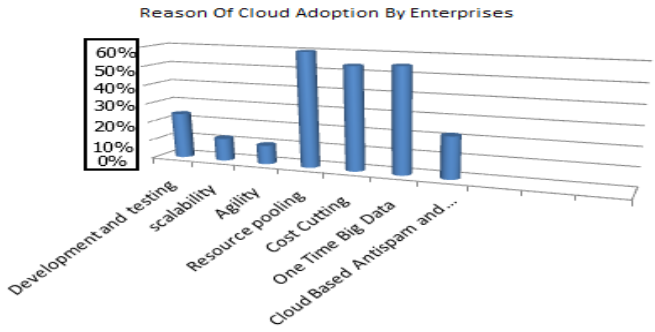

Fig II Adoption reasons for cloud by small medium enterprises (SMEs) [4].

A. Cloud has four deployment models corresponding to these services.

- Public cloud- the infrastructure available for all organization.
- Private cloud- the infrastructure for single organization.
- Community cloud- the infrastructure is share among organizations.
- Hybrid cloud- The infrastructure consists of two or more clouds either public or private or both cloud.

WAR AMONG DIFFERENT ORGANIZATION OF CLOUD COMPUTING

A. Taxonomy of giants.

Google has been a cloud company since its birth in 1998. It is best common known for its search service, but now hit all sorts of other products and services, too. It has made a global network of three dozen data centers with 2m servers, say some measure. Among more things, it makes a suite of web-based applications. Microsoft started on the ground level. Office, its bestselling suite of PC programs, is almost as everywhere as Windows. But the company is less a guest to cloud computing than it may seem. It has built a network of data centers, and is starting to gain traction after losing billions developing online services. Its Xbox games console has impressive online features. Bing, its new search engine, has achieved a shade in market share. Apple, too, came from outside the cloud. Online services have ever been a bit of an afterthought to what the company excels at: pricey but highly innovative bundles of hardware and software, of which the iPhone is only the current example. Its online offerings the iTunes store for music and video, the App Store now mobile applications, and MobileMe, a collection of online services were all originally meant to drive demand for Apple's hardware, but the firm's concern in the cloud has grown. Unfortunately for Google, it is equally unclear whether the better open player will gain, as Microsoft did last time. Many of Google's new services have failed to take off. Having curb by the software on the PC, smart-phones and other client devices, Microsoft can more easily setup what it calls "seamless experiences", for illustration by keeping a user's address book and another personal information in step. End user may also prefer Apple's hardly integrated, easy-to-use devices and services, even with the restrictions they enforce. Lots of people buy iPods and download music from iTunes even though it is difficult to play the songs on other devices.

B. Full war chests.

This means that all three will have ample resources to spend in the main areas of the fight: data centers, cloud services and the periphery. Now data centers, Google is leading, but Microsoft is taking up in size and sophistication. Apple has most to get, but this, too, look only a question of time and money. Just as much of hardware has become a products, knowing how to build huge data centers may not be a big competitive advantage for long. And data centers can get only so big before scale ceases to be an advantage. In services too, Google is ahead. But in Bing Microsoft may at last have found a worthy rival. The big question is whether Apple can catch up. Its iTunes and App stores are gainer, to be sure, but for now they are deeply specialized. The obvious candidates are Amazon, the world's huge online retailer, and Facebook, the best social network. Amazon at present has a cloud of array. It offers cloud computing services to other online firms and has advanced inflame, an electronic reader, which is due to be available worldwide from October 19th. Facebook [15] runs what is arguably the must be successful cloud service, along more than 300m registered users. It brings a platform for people to communicate, share information and cooperate online.

TABLE-I WAR AGAINEST GAINTS OF CLOUD[11].

How efficient cloud giants			
	APPLE	GOOGLE	MICROSOFT
Revenue	$34.6bn	$22.3bn	$58.4bn
Profit	$5.2bn	$4.6bn	$14.6bn
Employees	32000	19786	93000
Market capitalization	$170.2bn	$127.3bn	$230.4bn

IV. Barriers to Cloud Computing Adoption in the Enterprise.

Although there are many benefits to adopting cloud computing, there are also some powerful barriers to adoption. Two of the most powerful barriers to adoption are security and privacy, and we discuss them broadly in the following topics. However, it is important to at least call out what some of the other barriers to adoption are, and we discuss those in the following sections.

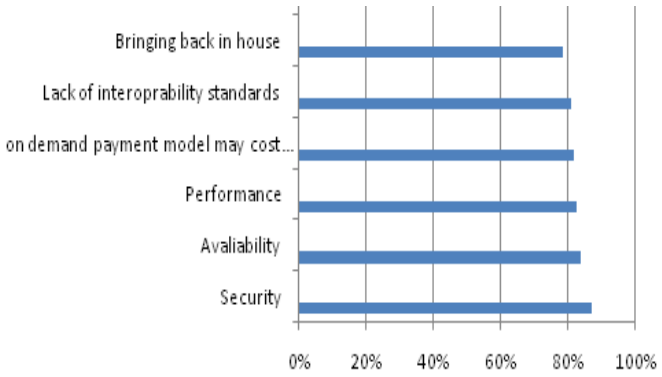

Fig.III Issues in cloud adoption [40].

- Security.
- Privacy.
- Connectivity and Open Access.
- Reliability.
- Interoperability.
- Independence from CSPs.
- Economic Value.
- IT Governance.
- Changes in the IT Organization.
- Political Issues Due to Global Boundaries.

Political Issues Due to Global Boundaries.

In the cloud computing world, there is variability in terms of where the physical data resides, where processing takes place, and from where the data is accessed. Given this variability, Different privacy rules and regulations may apply. Because of these varying rules and regulations, by definition politics becomes an element in the adoption of cloud computing, which is effectively multijurisdictional. For cloud computing to continually evolve into a borderless and global tool, it needs to be separated from politics. Currently, some important global technological and political powers are making laws that can have a negative impact on the development of the global cloud. It was instrumental in crunching the massive amounts of data needed to complete the Human Genome Project. That project has netted answers to the question of where hundreds of diseases and traits come from, and would not have been possible in such a short time without the computer sharing allowed by cloud computing and available via the Internet [40].

V. What Are the Key Privacy Concerns in the Cloud?

Privacy advocates have raised many concerns about cloud computing. These concerns typically mix security and privacy. Here are some Political considerations to be aware of:

B. Access

Data subjects have a right to know what personal information is held. In the cloud, the main concern is the organization's ability to provide the individual with access to all personal information, and to comply with stated requests.

C. Compliance

What are the privacy compliance claim in the cloud, what are the applicable laws, regulations, standards, and contractual commitments that govern this information, and is any responsibility for maintaining the compliance.

D. Storage

Where is the data in the cloud stored? Was it transferred to another data center in another country? Is it commingled with information from other organizations that use the same CSP?

E. Retention

How long is personal information (that is transferred to the cloud) retained? Which retention policy controls the data? Does the organization own the data, or the CSP? Who enforces the retention policy in the cloud, and how are exceptions to this policy (such as litigation holds) managed?

F. Destruction

Cloud storage providers usually replicate the data across multiple systems and sites increased availability is one of the benefits they provide. This benefit changes into a challenge when the organization tries to destroy the data that can truly destroy information once it is in the cloud? Did the CSP really damaged the data, or just make it inaccessible to the organization? Is the CSP care the information longer than necessary so that it can mine the data for its own use?

G. Audit and monitoring

How can End user monitor their CSP and provide assurance to relevant stakeholders that privacy requirements are met when their Personal information is in the cloud?

H. Privacy breaches

How do end users know that a breach has occurred, how do they ensure that the CSP notifies, when a breach occurs, and who is responsible for managing the breach notification process (and costs associated with the process)? If contracts include liability for breaches resulting from negligence of the CSP, how is the contract enforced and how is it determined

who is at fault? Many of these concerns are not specific to personal information, but to all types of information and a broader set of compliance requirements.

VI. WHO IS RESPONSIBLE FOR PROTECTING PRIVACY?

There are conflicting opinions regarding who is responsible for security and privacy. When an organization loses control of users' personal information, the users are responsible (directly or indirectly) for subsequent damages resulting from the loss. Organizations can transfer duty, but not accountability.

- Risk assessment and mitigation all over the data life cycle is critical.
- Knowledge about legal obligations and contractual agreements or commitments is imperative.

There are, however, many new risks and unknowns; the overall complexity of privacy Protection in the cloud represents a bigger challenge.

CHANGES TO PRIVACY RISK MANAGEMENT AND COMPLIANCE IN RELATION TO CLOUD COMPUTING

The following topics describe analysis of the potential impact of cloud computing on the key OECD (Organization for Economic Cooperation and Development) and other common privacy principles [29], [30].

- *Collection Limitation Principle*.

This principle specifies that collection of personal data should be limited to the minimum amount of data required for the purpose for which it is collected. In the privacy arena, lack of specifics on data collection with providers creates misunderstandings down the road. There are comprehensive security frameworks and standards (such as the ISO 27000 series, NIST guidelines, etc.), and organizations know how to implement them. There is no universally adopted privacy standard. It is essential that service-level agreements (SLAs) are initially defined before any information is provided or shared.

- Use Limitation Principle.

This principle specifies that personal data should not be leak, made available or otherwise used for purposes other than those with the consent of the data subject, or by the authority of law. Cloud computing places a diverse collection of user and business information in a single location.

- *Security Principle.*

Security is one of the key requirements to enable privacy. This principle specifies that personal data should be protected by reasonable security safeguards against such risks as loss or unwanted access, destruction, use, modification, or disclosure of data.

- *Retention and Destruction Principle.*

This principle specifies that personal data should not be retained for longer than needed to perform the task for which it was collected, or as required by laws or regulations. Most policies have been driven or imposed by legislation and control, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Sarbanes-Oxley Act (SOX), and other federal and state compliance requirements. The actual deletion process is sometimes almost defined. But when data copies, data backups, or archives are erased, are they really gone?

- *Transfer Principle.*

This principle specifies that data should not be transferred to countries that don't provide the same level of privacy protection as the organization that collected the information. In a cloud computing environment, infrastructure is shared between organizations; therefore, there are threats associated with the fact that the data is stored and processed remotely, and there is increased sharing of platforms between users, which increases the need to protect privacy of data stored in the cloud. Another feature of cloud computing is that it is a dynamic environment; for example, service interactions can be created in a more dynamic way than in traditional e-commerce. The transfer challenge is further complicated because data can be anywhere in the world usually, a company computing in the cloud does not know in what country its data resides at any given time. Instead of its data being saved on the company's servers, data is stored on the service provider's servers, which could be in Europe, China, or anywhere else, they all are have their own law to handle.

- *Accountability Principle.*

Accountability within cloud computing can be achieved by attaching policies to data and mechanisms to ensure that these policies are adhered to by the parties that use, store, or share that data, irrespective of the jurisdiction in which the information is processed. The way to move onward is for organizations to value accountability and build mechanisms for accountable, responsible decision creating while handling data.

VII. LEGAL AND REGULATORY IMPLICATIONS.

Across the globe, the legal and regulatory requirements for data privacy range from strictly enforced to non-existent, which can prove to be a daunting challenge for multinational companies or those serving customers from multiple jurisdictions. Some programs such as the OECD Guidelines and the European Union Data Protection Directive are principle-based, where personal data processing is not permitted, except as directed in the statutes, whereas in countries such as the United States, certain types of processing are restricted, but activities are generally considered lawful unless specifically prohibited by

applicable state and federal regulations. The jurisdiction of these laws is determined differently in different countries and states. Some of the laws are based on the location of the organization, some on the physical location of the data center, and some on the location of the data subjects. The only universal consistency is that the law has not caught up with the technology. To further compound the challenge of processing personal data in a global environment, some requirements are conflicting. For example, compliance with the U.S. Federal Rules of Civil Procedure (FRCP) can breach the EU Directive. Differing attitudes on privacy have been the force behind countless cross-jurisdictional legal battles, international trade barriers, and longstanding political disputes. In the next section, we will describe the implications of cloud computing on compliance with various privacy regulations. The scope is limited to aspects that are different in a public cloud environment, because many resources are available to help understand the full extent of the requirements [40].

1) Federal Rules of Civil Procedure.

Rule 26 of the FRCP requires that parties involved in a civil lawsuit have a duty to disclose to the other party all information that will be used to support its claims or defenses. Clearly, a records management strategy addressing archiving and secure data destruction is essential to reducing the burden of compliance. According to Rule 34(a)(2)(E)(i) of the FRCP, electronically stored documents must be produced in the form in which they are kept in the normal course of business. Cloud computing environments often do not have the capability to support hold requirements in a way that both segregates the information subject to the hold and does not share information that is related to other individuals, causing a potential violation of the individuals' privacy and violation of privacy laws and regulations [40].

2) USA Patriot Act.

Perhaps the most controversial privacy-related legislation, the USA Patriot Act has several implications for cloud computing.

At a high level, the challenge with the Patriot Act can be viewed as location, location, location [7], [8]. [20]

3) Electronic Communications Privacy Act.

Fundamental to addressing all cloud computing risks (including those related to privacy) is the contractual agreement with the provider. It is absolutely critical for users to have a thorough understanding of the terms and conditions from both a legal and a technical perspective. Agreements should clearly describe the services provided, limitations, liabilities, and rights of each party. SLAs, contractual clauses, and a high-level understanding of applicable legislation can give user organizations, as well as data subjects, a false sense of security with regard to their rights to privacy [20].

4) FISMA.

The first thing to note when discussing the U.S. Federal Information Security Management Act of 2002 (FISMA) is that the act requires only U.S. federal agencies to develop, document, and implement an agency-wide information security program. It does not desire this of state agencies or quasi-governmental agencies, such as the U.S. Postal Service; yet, a contractor or other organization acting on behalf of a federal agency is also subject to FISMA, which is where the privacy implications of employing cloud computing begin to reveal themselves [20].

5) GLBA.

There are two key pieces to the Gramm-Leach-Bliley Act (GLBA) to consider when discussing the privacy implications of computing in the cloud: the Financial Privacy Rule and the Safeguards Rule. The Financial Privacy Rule requires financial institutions to provide their customers with a privacy notice upon inception of the relationship and annually. The privacy notice charge explain information collection, sharing, adoption, and protection. GLBA also requires that the notice give a financial institution's customer the right to opt out of the information being shared with unaffiliated parties.

6) HIPAA.

One of the key privacy implications of the United States when using the cloud is similar to that already faced by health care providers using non-cloud third-party vendors for data storage.

HIPAA regulates the use and disclosure of protected health information (PHI) by health care providers and health plans, but does not currently regulate their third-party providers. Organizations subject to HIPAA are required to enter into a business associate agreement with the third-party providers to transfer PHI, and this legally binds the providers to effectively be subject to HIPAA regulations. However, this agreement typically covers the transfer of data from the health plan organization to the CSP.

7) HITECH Act.

In early 2009, HIPAA was amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, a section of the American Recovery and Reinvestment Act of 2009 relating to health information technology. The goal of the law is, with others, to drive a transition to electronic health records (EHRs) so that by 2014 all U.S. residents will have an EHR. The law provides a privacy and security framework and safeguards to establish public trust so that individuals accept EHRs [20].

8) International Laws and Regulations.

The international regulatory environment is driven by two approaches: one represented by EU Directive 95/46/EC on the protection of individuals with regard to the processing of

personal data and on the free movement of such data (EU Directive), that was the model used by countries in Europe as well as Canada, and another reflected by the APEC Privacy Framework. The two approaches have a different privacy impact on cloud computing environments [42].

9) Eu Directive.

The most significant difference between the EU and U.S. legislation is the notion of personal privacy. In Europe, privacy is considered a basic human right and cannot be divorced from one's personal freedom. The EU Directive compels member states to implement and enforce data privacy legislation (national law) that (at a minimum) satisfies the requirements set forth in the EU Directive (community or supranational law). Processing of personal data is prohibited, unless it is in compliance with both sets of applicable regulation. The EU Directive contains several provisions to allow transfer of data, including (among others):

• The data subject has given his consent truly to the proposed transfer.

• The transfer is basic for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request.

• The transfer is basic for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party.

• The transfer is basic or legally required on important public interest grounds, or for the establishment, exercise, or defense of legal claims.

• The transfer is basic to protect the vital interests of the data subject.

The EU Directive's guidance on this matter is that the controller must, point to processing is carried out on his behalf, select a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must secure compliance with those measures. Complying with this set of guidelines does not necessarily imply compliance with the EU Privacy law. Similar to the federal or state jurisdictions in the United States, EU member states must implement these laws locally, as a minimum effort. Each state has drafted its own legislation, and some are even more stringent than the supranational law. It is advisable to consult legal counsel when determining which stipulations must be adhered to. The stringent requirements of the EU Directive may present legal limitations on the adoption of cloud computing, requiring organizations to increase the level of scrutiny on CSPs [30].

10) APEC Privacy Framework.

The Asia Pacific Economic Corporation (APEC) Privacy Framework, similar to the OECD Privacy Guidelines, is established as best practices for organizations operating within these economic areas. Unlike the EU Directive, these guidelines are not mandatory, and as such they may be adopted by participating economies as part of their laws. There is currently a significant effort by key APEC economies to drive broad adoption of the framework. Based on this effort, it is our view that any organization processing personal data will benefit from adherence to the framework. The APEC Privacy Framework is implemented via a pilot (pathfinder) led by multiple economies within the region. The pilot involves both governments and private sector organizations, and should provide a consistent approach for data transfer within the region. Successful implementation of the framework can provide a stronger basis for CSPs to operate seamlessly across borders. These guidelines will provide a more flexible environment that supports transition to a cloud environment, where data flows between economies.

VIII. CONCLUSION

This paper has described several dark fears and vague surmises about cloud computing. However, it is likely that a combination of technical solutions, business practices, and standard contracts between service providers and customers will be able to resolve most if not all of them. While using cloud computing services for Easter egg business, it will be the service provider's responsibility to maintain, patch and upgrade the servers on which these services run. The services will likely be accessible from anywhere with Web access (although there may be geographical or other restrictions for legal reasons). If more orders for Easter eggs arrive than were expected, the burden of rapidly finding the additional computing resources to process the orders will be taken by the service provider, not by the end user. For subcontractors, cloud computing hit a whole new market. For vendors of computing services, the advantages include the possible for higher margins and for advertising revenue. They also may see hike in the size of the market for computer services, because cloud computing makes viable some small business models which would have tackle in its absence. Finally, cloud computing may provide a good source of income for lawyers.

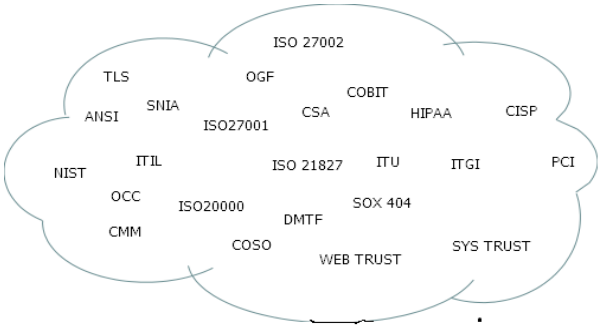

Fig. IV wwcb (Worldwide cloud boundaries)

REFERENCE

[1] B Thompson, "Storm Warning for Cloud Computing" (2008)Available athttp://news.bbc.co.uk/2/hi/technology/7421099.stm (accessed 23 Mar 2009).

[2] Gartner, Inc, "Gartner Highlights 27 Technologies in the 2008 Hype Cycle for Emerging Technologies" (2008) available at http://www.gartner.com/it/page.jsp?id=739613 (accessed 23 Mar 2009).

[3] D Gottfrid, "Self-service, Prorated Super Computing Fun!" (1 Nov 2007) available at http://open.blogs.nytimes.com/2007/11/01/self-service-prorated-super-computing-fun/ (accessed 23 Mar 2009).

[4] The New York Times, "The Hound of the Baskervilles. Did it Slay Sir Charles?"(29Mar1902) available at http://query.nytimes.com/mem/archivefree/pdf?res=9502E0D9103BE733A2575AC2A9659C946397D6CF (accessed 23 Mar 2009.

[5] A Conan Doyle, The Hound of the Baskervilles (London: Penguin Books, Red Classics edition,2007), at 187.

[6] Follorou, "La complainte du Blackberry dans les ministères" (2007), *Le Monde*, 20 Jun 2007.

[7] D Fraser, "The Canadian Response to the USA Patriot Act" (2007) 5 *IEEE Security and Privacy* no.5,66-68, availableat http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04336282 (accessed 23 Mar2009).

[8] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept andObstruct Terrorism (USA PATRIOT ACT) Act 2001*, Title V, s 505.

[9] *Regulation of Investigatory Powers Act 2000*, Part II, s 28.

[10] J Madelin, "Transformational Change – large converged networks come to life" (2008), Adaptive and Resilient Computing workshop, London, 30 Sept 2008.

[11] A Liptak, "A Wave of the Watch List, and Speech Disappears" *New York Times*, 4 Mar 2008 available at http://www.nytimes.com/2008/03/04/us/04bar.html (accessed 23 Mar 2009).

[12] Barr, Cloud Computing session, BarCamp Brighton 2, Falmouth, 13-15 Mar 2008.

[13] Fail Whale Fan Club, "The Fail Whale Fan Club: celebrating Twitter and our favourite error page cetacean" (2008-2009) available at http://failwhale.com/ (accessed 23 Mar 2009).

[14] Facebook, "FailWhale" (2009) available at http://www.facebook.com/pages/FailWhale/64467830480 (accessed 23 Mar 2009).

[15] Yahoo!, "flickr: Eve Whale" (2009) available at http://www.flickr.com/photos/crispy_chips/2622841707/#comment72157606109949329 (accessed 23Mar 2009).

[16] Google, "Welcome to Google Apps: Google terms of service"(2009)available at http://www.google.com/apps/intl/en/terms/user_terms.html (accessed 23 Mar 2009).

[17] Amazon Web Services LLC, "AWS Customer Agreement" (2009) available at http://aws.amazon.com/agreement/ (accessed 23 Mar 2009).

[18] P Massey, "Privacy, Regulation, Security and Cloud Computing", Powered By Cloud, London, 2-3Feb 2009.

[19] United Nations Convention on Contracts for the International Sale of Goods (1980), art 35

[20] Salesforce.com, "Master Subscription Agreement" (2000-2009) available at http://www.salesforce.com/company/msa.jsp (accessed 23 Mar 2009).

[21] J Jones, "Data Diligence" (2005) *ComputerWorld*, 14 November 2005 available at http://www.computerworld.com/managementtopics/management/story/0,10801,106127,00.html(accessed 23 Mar 2009).

[22] Amazon Web Services LLC, "Amazon S3 Service Level Agreement" (2009) available at http://aws.amazon.com/s3-sla/ (accessed 23 Mar 2009).

[23] Amazon Web Services LLC, "Amazon EC2 Service Level Agreement" (2008) available at http://aws.amazon.com/ec2-sla/ (accessed 23 Mar 2009).

[24] J Brodkin, "More outages hit Amazon's S3 storage service" *NetworkWorld*, 21 Jul 2008 available at http://www.networkworld.com/news/2008/072108-amazon-outages.html (accessed 23 Mar 2009).

[25] J Salmon, "Clouded in uncertainty – the legal pitfalls of cloud computing" (2008) *Computing*, 24Sept 2008 available at http://www.computing.co.uk/computing/features/222601/clouded-uncertainty-4229153 (accessed 23 Mar 2009).

[26] Google, "What does a Google Apps SAS70 Type II audit mean to me?" (27 Jan 2009) available at http://www.google.com/support/a/bin/answer.py?hl=en&answer=138340 (accessed 23 Mar 2009).

[27] K Greene, "Google's Cloud Looms Large" (2007) *MIT Technology Review*, 3 Dec 2007 available at http://www.technologyreview.com/business/19785/page2/ (accessed 23 Mar 2009).

[28] M Crandell, "RightScale: the cloud management platform" (2009) Powered by Cloud, London, 2-3Feb 2009.

[29] D Lupafya, panel session at Powered by Cloud, London Feb 2-3 2008.

[30] J Vincent, "Prophet: a path out of the cloud" (2008), Open Source Convention (OSCON), Portland OR, 21-25 July 2008 available at http://assets.en.oreilly.com/1/event/12/Prophet,%20your%20path%20out%20of%20the%20cloud%20Presentation.pdf (accessed 23 Mar 2009).

[31] D Raywood, "Google admits that some of its Docs have been accidentally shared" (2009) *S C Magazine*, 10 Mar2009availableathttp://www.scmagazineuk.com/Google-admits-that-some-of-its-Docs-have-beenaccidentally-shared/article/128491 (accessed 23 Mar 2009.

[32] A Greenberg, "Cloud Computing's Stormy Side" (19 Feb 2008) available at http://www.forbes.com/2008/02/17/web-application-cloud-tech-intel-cx_ag_0219cloud.html (accessed 22 Mar 2009).

[33] N Dhanjani, "Amazon's Elastic Compute Cloud [EC2]: Initial Thoughts on Security Implications"(28 April 2008) available at http://www.dhanjani.com/blog/2008/04/index.html (accessed 23 Mar2009).

[34] V Pai et al, "The Dark side of the Web: An Open Proxy's View" (2004) 34 *ACM SIGCOMM Computer Communication Review* issue 1, 55-62 available at http://portal.acm.org/citation.cfm?doid=972374.972385 (accessed 23 Mar 2009).

[35] A Narayanan and V Shmatikov, "Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)" (2008) IEEE Symposium on Security and Privacy (S&P),Oakland CA, 18-21 May 2008, available at http://arxiv.org/PS_cache/cs/pdf/0610/0610105v2.pdf(accessed 23 Mar 2009).

Authors Profile

Mr. Saroj Kumar, PhD Scholar from Maharishi University of Information Technology, Lucknow had completed his M.Tech form NIT - Allahabad and served more than 10 year in academic in different colleges in India.

Dr. Santosh Kumar,Associate Professor and Head in Maharishi University of Information Technology, Lucknow. Serving more than 10 year in Academic Field and Guided more than 10 PhD Scholar in Computer Science Dpartment

