Technical Impediments to Cloud Computing: A Survey

Praveen Kumar Rao K
Assoc Prof & Head,
Department of CSE,
KITS, Singapur, Huzurabad,
Karimnagar.

Gowtham Kumar N
Assistant Professor,
Department of CSE,
KITS, Singapur, Huzurabad,
Karimnagar,

Raghu N
Assistant Professor,
Department of CSE,
KITS, Singapur, Huzurabad,
Karimnagar,

ABSTRACT

Cloud computing is a term that they come across often these days. Many Companies are often trying to increase the functionality of Information Technology while minimizing capital expenditures. This paper presents the survey on primary impediments to cloud computing while adopting, based on the cloud services, which are requested by the cloud customer. Mainly this survey focus on the issues related to security, interoperability, regulation policy, reliability, complexity. This paper is also suggested some necessary guidelines for regulation compliance in cloud computing.

Keywords

Cloud computing, Cloud vendor, SLA, GRC, Tightly coupled & loosely coupled systems.

I. INTRODUCTION

Cloud computing services allow individuals and businesses to use software and hardware that are maintained by third parties at remote locations. There are some cloud services include, social networking sites, webmail, online file storage and online business applications. By using cloud computing system user can access to information and resources from anywhere that a network connection is available. Cloud computing comprise data storage space, networks, system processing power, and specialized business and user applications and furnish a shared pool of resources.

Recently cloud services are popular because they can reduce the cost and complexity, since cloud users do not have to invest in IT infrastructure, no need of purchase hardware and software licenses, the advantages are low up-front prices, quick return on investment, quick deployment, customization, elastic use, and solutions that can make use of new ideas [5]. Apart from this, cloud providers that have specialized in a particular area (such as e-mail) can bring advanced services that a single company might not be able to afford or implement.

The cloud is reliable in that it can able access to applications and documents from anywhere in the world through the Internet. Cloud computing is often considered capable because it allows organizations to free up resources to focus on innovation and product implementation [2]. Another benefit of cloud is that personal information of user may be better protected. Exclusively, cloud computing may need improve efforts to build privacy protection from the start and make use of better security mechanisms. Cloud computing will make able more flexible IT acquisition and improvements based on the sensitivity of the data.

Pervasive use of the cloud may also encourage open standard protocols for cloud computing that will establish baseline information security features common across different services and service providers. In addition for better audit trails, cloud computing may become as an option [1].

1. Service Models

The cloud computing offers several service models comprise Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [1]. In Software as a Service model, offers an application that already developed, provided with any required software, hardware, operating system and network. In PaaS, the hardware, an operating system, and network are provided, and the customer has to installs or develops his own software and applications. The IaaS model just furnishes the hardware and network; the customer installs his own operating systems or develops software and applications [3].

2. Deployment of Cloud Services

Cloud services are typically made available over a private cloud, public cloud or hybrid cloud, community cloud as in Figure 1 [5].

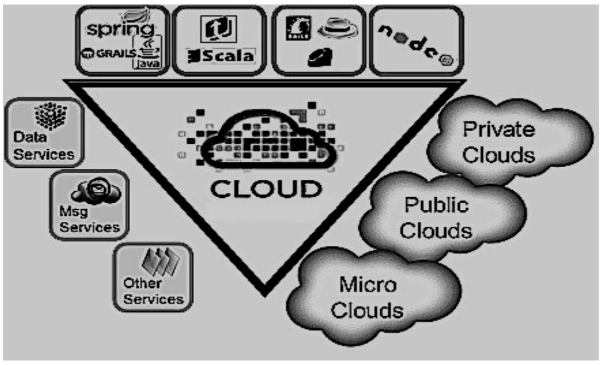

Figure 1: Cloud Services Types

In a **Public Cloud** are offered services over the Internet and are owned and operated by a cloud provider. Some examples comprise services focus on the general public, such as social networking sites, online photo storage services, or e-mail services. However, business services can also be offered in a public cloud [1].In a **Private Cloud**, individual operated and maintained the cloud infrastructure for a specific organization, and is managed by the same organization or a third party. In a **Community Cloud**, several organizations shared the service and made available only to that organization. The infrastructure may be owned and controlled by the organizations or by a cloud service provider. A **Hybrid Cloud** is a combination public and community clouds.

To the adoption of cloud computing, Cloud customers need to consider the primary impediments in order of importance to consumers of cloud based services such as security, interoperability, regulatory policies, reliability, and complexity. These concerns elevate contract drafting issues for cloud computing contracts.

II. TECHNICAL IMPEDIMENTS

1. Potential Privacy Risks – Security

There are privacy and security concerns too, where there are benefits. Data is moving through the Internet and is stored in diversified locations. In addition, cloud providers often serve multiple customers at the same instant. All of this may increase the scale of exposure to possible breaches, both accidental and purposeful.

Concerns have been arise by many that cloud computing may lead to "function crawl" that uses of data by cloud providers that were not predicted when the information was originally collected from data sources and for which agreement has not been acquired. There is small incentive to remove the information from the cloud, given how inexpensive it is to keep data, and more reasons to find other things to do with it.

Security issues, the need to separate data when dealing with cloud providers that serve multiple customers, contingent secondary uses of the data—these are areas that organizations should keep in mind when considering a cloud provider and when agreements contracts or reviewing terms of service with a cloud provider [3]. The organization transferring this information to the provider is eventually accountable for its security, it needs to make sure that the personal information is appropriate handled.

Privacy is not a breach but it must be taken into account. The *Personal Information Protection and Electronic Documents Act* (PIPEDA) does not inhibit an organization from transferring personal information to an organization in another jurisdiction for processing. Nevertheless, PIPEDA set up rules governing those transfers particularly with respect to acquiring consent for the collection, make use and reveal of personal information, protecting the data, and make sure accountability for the information and transparency in terms of practices [7].

These considerations apply whether moving data in the cloud or otherwise. It is essential to note that many cloud service providers other than Canadian based may also be subject to PIPEDA. The extent that a cloud provider has a real and essential connection to Canada, and assemble, uses or discloses personal information in the course of a commercial activity, the cloud provider is expected to provide security personal information, in preserving with PIPEDA.

Service level agreements (SLAs) should comprise provisions indicating the infrastructure and security for the cloud service. The customer should specify the security parameters and security monitoring assurance by the service provider in the SLA in specific and measurable ways. Without these specifics, it will be difficult to estimate security and to know whether the service provider is disseminating the security assurance [4]. For example, provisions commonly describe what intrusion monitoring and incident reporting the customer will provide. The SLA may also furnish the customer with the ability to periodically audit the security of the provider.

Recent surveys specifies that many customers of cloud services do not observe security aspects of their cloud computing services on a uninterrupted basis, irrespective of security being a top concern for respondents. Availability is frequently addressed in the SLA and observed by the customer for example. Other security parameters are often not well-covered in the SLA or, if covered, are not monitored much enough. For example, if the SLA supply for penetration tests, failover or backup testing, the consumer should develop a program to make sure the testing is actually performed and the results are reported. The program should be overlayed in the SLA [4]. Data portability testing is another issue is often overlooked and not tested. Security and testing in all cases reports should be reviewed and retained in case a problem implementation.

Also survey considered whether there should be penalties for noncompliance. Many SLAs comprise detailed security definitions and observation, but no specific cater to addressing the outcomes for failing to comply. Smooth provisions addressing security breaches of the contract are often too general to provide meaningful remedies for barrier of the SLA. Compliance and penalty caters should be crafted to incentivize the vendor to provide the required service level.

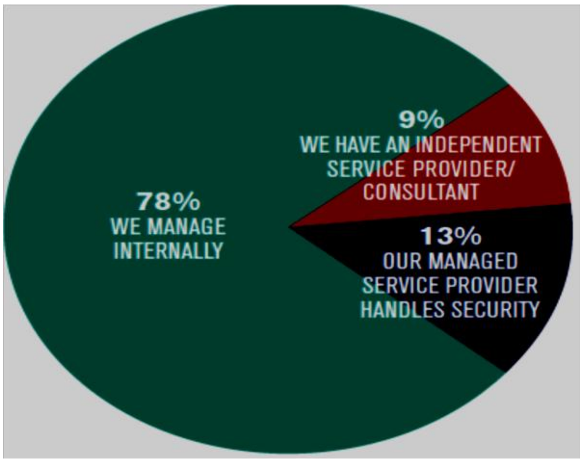

Figure 2: Cloud Security Responsibility

Responsibility for the data and management of cloud is left to the organization only. Overwhelmingly, survey respondents report that their organizations approximately 78 % are managing cloud security internally.13% organization said they use a Managed Service Provider (MSP) and only 9% said they utilize independent service providers or consultants shown in Figure 2. Some respondent's clarify that responsibility for their organizations' cloud security is shared between internal resources and external providers [6].

2. Interoperability

The interoperability of information between private clouds and public clouds are critical enablers for vast adoption of cloud computing by the business organizations. Many organizations have made considerable progress toward standardizing their data, processes, and systems over the development of ERPs. This process has been enabled by scalable infrastructures to create single instances, or highly integrated connections among instances, to maintain the consistency of master and transaction data and produce reliable consolidated information.

The speed at which businesses change may still outpace the ability of IT organizations to respond to these changes, even with these developed platforms, SaaS applications disseminate through the cloud provide fast-deployment, with a low-capita option [8]. It is critical to integrate with conventional applications that may be resident in a separate cloud, depending on the application. The standard for interoperability is either a barrier or an enabler to interoperability, and permits maintenance of the steadiness and integrity of a company's information and processes.

3. Regulatory Compliance

Cloud computing makes it harder for business to be sure they're consent with industry and government regulations. IT and legal experts provides CIOs advice on how to stay in compliance even when their applications abide in the cloud [17].

Cloud computing look like simple in concept, and to be sure, simplicity of operation, deployment and licensing are its most attractive assets. But when it comes to questions of policies, once the customer scratch the surface, find more questions and more to think about than ever before. Compliance covers a lot of ground, from government regulations such as the European Union Data Protection Act, and Sarbanes-Oxley to industry regulations such as PCI DSS for payment cards and HIPAA for health data. If the customer moving to a public-cloud infrastructure platform, users are ready to giving up some controls of a cloud-based application suite to the cloud vendor, may have internal controls in place [18].

Today many auditors and CEOs want to know how to leap into cloud computing in a way that preserves their good standing in regulatory compliance. Here are four guidelines for keeping tabs on policies in the cloud, from analysts, consultants and vendors.

3.1 Realize of new challenges the cloud may add to the IT workload.

At the time of assessment of cloud vendors, users start by looking for high practices and complex strategies for identity, access management, and incident response and data protection. These are the constructive requirements for compliance in regulations. The Cloud users will likely to face some cloud-specific challenges, as and when users map specific compliance requirements to his prospective cloud vendor's controls. Data location is become one issue. The EU Data Protection Act, strives to keep personal information within the European Union, for example. To comply, cloud vendor should keep European customer data on servers located in Europe [3].

Multi-tenancy and de-provisioning also present challenges. Multi-tenancy used by public cloud providers to improve the efficiency of server workloads and remain costs down. But multi-tenancy means users sharing server space with other businesses, so they should know what protection methods that the cloud provider has in place to prevent any compromise. Users may also want to use encryption depending on how critical their data is. HIPAA, for example, requires that all user data, both moving and at rest, be encrypted. Because of password-authentication methods grow in complexity and volume user de-provisioning is an issue that will become more challenging. Federated identity management methods make able it easier for users to log on to multiple clouds, and that will lead de-provisioning much difficult toughest task.

3.2Track the fast-changing standards landscape

Decisions about what applications to move to the cloud and when to move them will benefit from an understanding of new and/or modified standards that are now evolving for cloud computing. Today users can look for SAS 70 Type II and ISO 27001 certifications for general compliance with controls for financial and information security typically in accordance with government and industry rules, but these don't guarantee that customer's company processes will comply.

Standards like ISO 27001 and SAS 70 are helpful but they're point-in-time and these standard are not very specific when it comes to data security, identity management, administrator control, things like that, and is more visibility to the users is needed about what's going on. Cloud Security Alliance, provides development of standardized auditing frameworks to facilitate communication between users and cloud vendors. CSA is a three-year-old organization which is gaining popularity in rapid way among users, auditors and service providers.

Well underway, for example, is a governance, risk and compliance (GRC) standards suite, which has four main elements[9]: the Cloud Trust Protocol(mechanism by which cloud service consumers ask for and receive information about the elements of transparency as applied to cloud service providers), Cloud Audit(to provide a common interface and namespace that allows enterprises who are interested in streamlining their audit processes), Consensus Assessments Initiative (offers a detailed questionnaire that maps those control areas to specific questions that users and auditors can ask cloud vendors) and the Cloud Controls Matrix (includes a spreadsheet that maps basic requirements for major standards to their IT control areas, such as Human Resources, Personnel Termination).

In the next several years, due to the efforts of the CSA and other alliances, and those of industry groups and government agencies are tied to produce a wealth of standards. ISO, ITU and NIST groups have formal alliances with CSA, so that its developments can be used by those groups as contributions to standards they're working on. 48 industry groups working on security-related standards counted according to 2010 Forrester Research report [10].

3.3 Take care with the SLA

Don't assume cloud vendor's standard terms and conditions will fit user's requirements, in spite of of their company's size or status. User's have to scrutinize the vendor's contract carefully [11], advice which has given by Hogan Lovells[an international law firm] having the experience in cloud compliance and security issues. And Michael Larner, an attorney, who always help to the clients in the negotiation of Service Level Agreements (SLAs), try to explains the user's own risk-benefit analysis to see if the vendor's standard contract is sufficient for their compliance needs. Otherwise, decides what they need to negotiate to increase user's comfort level.

Cloud computing make it more difficult for enterprises to be sure they're following with industry and government regulations. IT and legal experts provides CIOs advice on how to stay in compliance even when their applications reside in the cloud. Customer company's size can give you leverage to reach an agreement, but a smaller business can find leverage, too, if it portray a new industry for a cloud vendor that wants to expand its market. Don't be afraid to negotiate in any case. With too many companies there's an assumption if you're dealing with a large vendor that the vendor won't negotiate. In fact, you need to find that whether the vendor is willing to make some exceptions to increase customer's comfort level or not [12].

If the users are new to the cloud, they may find that starting out with non-critical data on a pilot basis, is a good way to build confidence [11]. But due diligence doesn't end with a comprehensive SLA. Nirav Mehta, director of RSA's corporate strategy for cloud computing, says that it is better to watch the vendor closely. Even the users may have a good SLA, but if the vendor's cloud goes down, this may affect the business continuity in the future. In this case best strategy might be to use multiple clouds for backup assurance.

3.4 Make security a priority

To best understand potential risks and benefits, users should bring their security team into the conversation at the earliest possible opportunity. Security and compliance issues are brought up in the right contexts. It's important that business executives understand the security issues and can weigh the levels of risk against the budget they'll provide to mitigate some of those risks [17]

Moving to the cloud may offer an opportunity to align security with corporate goals in a more permanent way by formalizing the risk-estimation function in a security committee. The committee can help to estimate the risk and it also make budget proposals to fit customer's business strategy [3]. The cloud users should also pay attention to the security innovations coming from the numerous security services and vendor partnerships now growing up around the cloud. Dome9(Cloud security firewall management service), an Amazon partner, solves a cloud-specific technical problem that is closing secure-shell (SSH) and other ports of their cloud-based servers, an intruder who's already gained access to the cloud can't get in, when they're not in use.

Cloud computing may constitute some risks, but they'll likely detract as security innovations catch up. Even today, the security issues with cloud services don't worry most enterprise security teams as much as other IT trends, such as smart phone or social media proliferation. At the end, the security issue will be a speed bump, not a show-stopper, for cloud adoption [17]

4. Reliability in the cloud computing

Amazon's EC2(*Amazon* Elastic Compute Cloud) is probably the biggest fail story previously. But Microsoft's BPOS hosted bundle also experienced a significant amount of downtime year back. And, little monsters everywhere went irrational when Amazon released a digital copy of "Born This Way" for 99 cents, results Amazon to experience another unfortunate crash. These incidents have been covered extensively on the major tech news outlets, leading the technorati (Real time search for user generated media by tag or keyword) to once again question the reliability of cloud computing [15].

Many companies are affected, when things go awry in the cloud. Because these periods of downtime are public knowledge, it creates a misapprehension that cloud computing is unreliable and should be avoided. However, when things hesitate with on-premise systems, it is concealed behind the corporate curtain. It is still managing to get a bad rap, regardless of cloud compting's proven track record of success and gaining popularity as a cost-effective solution.

4.1 Downtime in the cloud

Anyone who wants to purchase a cloud-based software system is familiar with the Service Level Agreement (SLA). In the SLA, the provider consigns to a amount of time the system can be expected to run without interruption. Ideally this would be 100%, but as with most technology, hiccups in service delivery are necessary. Vendors take into account usually scheduled maintenance, and also unplanned outages or downtime, when creating the SLA. Most cloud companies can still quote about 99.9% up-time, after making those considerations [14]. That looks pretty impressive and seems to be in line with the kind of performance come to expect from SaaS vendors. It is unfortunate, according to naysayers still like to harp on that .1%.

Cloud customers still have the traditionalists that refuse to embrace the cloud, even though cloud systems are recognized as the cash-flow-friendly alternative to on-premise systems. Many prefer to instead reside on what if mission critical data is lost and what if the host's servers go down. For many on-site purists, what it really comes down to is control, while these are clearly valid questions. Cloud users feel more secure when they are in control of the system.

Walter Scott, CEO, GFI Software, however, specify that cloud-based solution vendors not only have the latest technology, the latest proxies(firewalls), the best data centers and the highest levels of redundancy possible but they will apply multiple layers of [in-depth defense] that users average business (a Fortune 500 company may be an exception) can never have.

4.2 Downtime on the ground

On-premise systems make promises on up-time, like their cloud computing counterparts. The difference is that when outages take place inside companies, customers typically don't hear about it. So the realization of the always-on on-premise model is skewed. This lack of coverage also makes it more difficult to track down any data considering the performance of on-premise systems. The Radicati Group, however, carry out a study in 2008 on on-premise email solutions that exposes some interesting points [14].

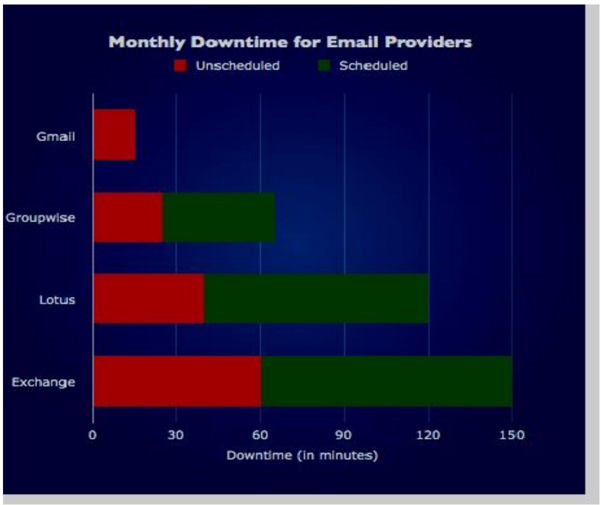

Figure 3: Monthly Downtime Report

Most notable in the findings is that among the most popular email systems (IBM Lotus Notes, Microsoft Exchange etc.) as shown in Figure 3, there was an average of 30-60 minutes of unscheduled downtime per month. Moreover, there was an average of 36-90 minutes of scheduled downtime. That maintains complete contrast to Gmail's total downtime of 10-15 minutes. Clearly, based on these findings, servers will lead to fail on occasion no matter where they are being hosted. According to the above chart, one might deduce that cloud companies are more capable of getting back online than companies that host their own servers.

4.3 Getting to 100%

There is one foreseeable upside to this negative press: it puts a fire under the backsides of cloud computing vendors to continually improve and stay on the moving toward the edge of technology.

Pombriant proposes better system modeling in the cloud. In another way, the structural design needs to be improved. The users are going to have to construct much greater reliability into their systems, if the users are going to have a truly robust and reliable infrastructure. Make use the advantage of electric utilities because they all have more generating capacity than is online at any one time as they take plants down, and then they also put them up. Electric utilities take away all of the apparent possibilities for failure. In this way that the cloud computing has to develop increasingly in the near future [15].

5. Cloud Computing and Complexity

The business of Information Technology (IT) has a complexity problem, before being implemented; it requires extremely specialized skills, multiple levels of translation and interpretation. This conceptual complexity creates a remarkable gap between business and IT leadership, but the most complex issue facing IT today is technology itself.

5.1. Time-to-Value

Time-to-Value is the most important metric according to dynamic, competitive service led economy but against this measure many corporate IT organizations unhappy and they fail miserably. The vital requirement for IT to keep pace with business speed has never been greater but the frightful reality for most CIOs is that the complexity of their IT infrastructures is drown beneath, in addition an increasing percentage of IT budgets are now exhausted on integrating and maintaining aging legacy systems rather than disseminating new value to the industry. There is no wonder most CEOs are dubious about the strategic value of IT.

Present legacy IT systems are inflexible, difficult to integrate and require a lot of effort and resources to transform to meet the needs of modern business strategies and service models. The cost of operating and maintaining these complex environments is unacceptably high, even the users successfully integrate multiple systems.

Many of the business IT systems operating today facing the problem known as "Era of Scarcity" which is the period until 2006 where program memory, computation, storage, and bandwidth were treated very limited and often incredibly expensive resources [19]. As a result of the resource economics of the "Era of Scarcity" the architecture of IT systems focused on steering and optimizing the resources used every layer of software in the architecture. During the "Era of Scarcity" an IT system designed can be likened to a finely crafted watch. Each part is precisely engineered and is highly optimized for its function and each part has a distinct role to play. The parts making up a pocket watch cannot easily be transformed into a wrist watch, so it is with most IT systems today.

Wrist watches and today's IT infrastructures are examples of *tightly coupled* systems. Each component of the system is designed and optimized to work only within a distinctive context. The force to high degrees of optimization means that parts cannot be shared or reused in other contexts. It also means that the failure of one part more often than not causes a failure of the entire system: *Tightly coupled* systems are often highly insubstantial. They are optimized within themselves but create significant friction when users try to use them in a broader context not anticipated by the original designers.

In order optimize the use of limited computing resources, the flooding complexity of most business IT infrastructures arose directly from the historic need to build *tightly coupled* systems. According to the present situation as an attempt to satisfy the needs of complex global business models there are many limitations of this *tightly coupled* approach are becoming abundantly clear. Most of the IT departments are today failing to deliver new capability at the rate demanded by the business is no surprise. The convolution and fragility of systems designed during the "Era of Scarcity" makes them not fit for purpose of the people are now entering in to the era.

5.2. Abundance and Opportunity

In 2006 Amazon launched their new "Amazon Web Services" business and placed a bet on the coming "Era of Abundance" when computing resources would be both cheap and *essentially* not limited. The economics of computing crossed a threshold in 2006. Storage, computation, and increasingly network bandwidth had become commodities. The Prices reduces and Amazon saw an opportunity to become the *de facto* utility provider of this new era, as the supply of available computational power outstripped demand. As was the case during the "Era of Scarcity" the new commodity economics of the "Era of Abundance" is driving a fundamental shift in IT systems architecture. This new approach to architecture is commonly referred to as "Cloud Computing."

If a tightly coupled approach to application and systems architecture was the optimal solution during the "Era of Scarcity" then the opposite loosely coupled approach is the defining characteristic of *abundant* cloud computing architectures. Abundant and inexpensive computing resources mean that systems today can be designed to be flexible from the start [16]. Recently cloud based applications are designed to scale elastically as user demand waxes and wanes. For providing better performance and reliability, new cloud based approaches to data storage keep multiple copies of data in different locations. Multiple layers of management software are used to decouple applications from the underlying infrastructure to improve scalability and reliability.

The use of APIs between system components is the key to building *loosely coupled* systems. This approach enables different systems designed independently to be rapidly integrated and re-configured as needed by the business. Individual building blocks can be replaced over time, because of the availability new technologies and better approaches. The systems based on cloud architectures are designed from the start to be both compatible and reconfigurable.

5.3. The Great Decoupling

The advent of the "Era of Abundance" and with it the emergence of new cloud computing architectures may very well offer a light at the end of IT's complexity tunnel. The ability to now design and construct a new generation of *loosely coupled* business systems based on cloud computing architectures offers the opportunity for IT departments to deliver scalable, reliable, flexible and agile solutions at a pace demanded by business leaders. The concept of *loose coupling* may turn out to be solvent that finally dissolves IT's historic complexity problem.

It's interesting to note that both mobile computing and Big-Data are also decoupling mechanisms. Mobile computing *decouples* information access and physical location. New approaches to Big-Data and analytics decouple the need to understand how data is structured from questions that will be asked over that data in the future. It is the *decoupling* effect of these technologies that makes them such powerful transformation tools [20]. Accomplishing the transformation from a complex, insubstantial and *tightly coupled* legacy environment to a new generation of scalable, agile, fault-tolerant *loosely coupled* systems will be the defining challenge for every CIO. As difficult as the transformation might be it is now not one that can be avoided, so the career of most CIOs will hinge on the outcome.

The "Great Decoupling" of IT based on the combination of cloud computing architectures, Big-Data analytics and mobile computing. The agility and flexibility of the systems that result from this will enable a fundamental transformation in the way customers do their business. The most powerful combination of *loosely coupled* business processes and IT systems will turn complexity from something, so users has to struggle to control and succeed into something they embrace and exploit**.**

6. CONCLUSION

This paper analyzed a few challenges on the way towards adopting the cloud computing, mainly the issues that are related to potential risks on diversified locations, security issues at the time of SLA, interoperability of information, regulation compliance during deployment and licensing, reliability in downtime and complexity in cloud computing. It is also suggested some guidelines in regulation compliance in cloud computing**.** This survey does not concentrate on the issues related to Vendor Locking, Privacy and Pricing.

REFERENCES

[1] Introduction to Cloud Computing Architecture White Paper 1st Edition, June 2009, Sun MicroSystem

[2] Srinivasa Rao V, Nageswara Rao N K, E Kusuma Kumari " Cloud Computing: An Overview" Journal of Theoretical and Applied Information Technology.

[3] Tharam Dillon, Chen Wu and Elizabeth Chang ""Cloud Computing: Issues and Challenges"2010 24th IEEE International Conference on Advanced Information Networking and Applications 1550-445X/10 $26.00 © 2010 IEEE DOI 10.1109/AINA.2010.187

[4] 4. Mun Choon Chan, Yow-Jian Lin, Xin Wang "A Scalable Monitoring Approach for Service Level Agreements Validation" IEEE International Conference on Network Protocols

[5] Sai Kiran M, Anusha A, Gowtham Kumar N3 Praveen Kumar Rao K "Selection Of Multi-Cloud Storage Using Cost Based Approach" International Journal of Computer and Electronics Research [Volume 2, Issue 2, April 2013].

[6] Cloud Security Survey 2013, AccelOps Survey

[7] A Guide for Individuals "Your Guide to PIPEDA" Office of the Privacy Commissioner of Canada

[8] Rajkumar Buyya, Saurabh Kumar Garg, and Rodrigo N. Calheiros" SLA-Oriented Resource Provisioning for Cloud Computing: Challenges, Architecture, and Solutions" 2011 International Conference on Cloud and Service Computing

[9] Evelyn Uhlrich Product Marketing, Software AG Martin Kling Business Development, Software AG "Governance, Risk and Compliance An Integrated Approach for Improving Oversight and Efficiency" February, 2012.

[10] Forrester Research 2010 Annual Report

[11] Winston Maxwell, Paris, France Christopher Wolf, Washington, DC 23 May 2012 "A Global Reality: Governmental Access to Data in the Cloud" A Hogan Lovells White Paper

[12] By Philip D. Porter and Michael E. Larner "Managing the Risk of Operating in the Cloud" Notational Association College and University Business Officers.

[13] "An analysis of security issues for cloud computing" Keiko Hashizume1*, David G Rosado2, Eduardo Fernández-Medina2 and Eduardo B Fernandez1 –Journal of Internet Services and applications.

[14] Cloud Computing Vulnerability Incidents: A Statistical Overview August 23, 2012; Revised March 13, 2013,Cloud Security Alliance

[15] "Cloud Computing in Retail: Evaluating the Case for Advanced SaaS" A Retail Touch Points White Paper

[16] Rafael Moreno-Vozmediano, Ruben S. Montero, Ignacio M. Llo Rente, "Multi-Cloud Deployment of Computing Clusters for Loosely-Coupled MTC Applications" Draft for IEEE TPDS (Special issue on many-task computing), July 2010

[17] Web-Application Architecture for Regulatory Compliant Cloud Computing Version 1.2 March 15, 2011, StrongAuth-Secure the core

[18] Mick Seals "HIPAA in the Cloud" Technical Architectures that Render PHI as Secured'-SOGETI

[19] Kenji E. Kushida, Jonathan Murray, John Zysman "Diffusing the Cloud: Cloud Computing and Implications for Public Policy" Springerlink.com

[20] Oracle JD Edwards Cloud Computing "Choosing a deployment strategy that fits" An Oracle White Paper October 2012