ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Challenges and Opportunities with Cloud Computing

Sandeep Kelkar

Assistant Professor, Prin. L. N. Welingkar Institute of Management Development and Research, Mumbai, India

ABSTRACT*:* Cloud computing is a model for providing computing service such as storage, servers, services and applications, without physically acquiring them via the internet. Access to such service could be free or pay as per use. So that the organizations does not have to spent time and cost in managing them. Many business institutions are moving towards the cloud computing due to the efficiency of services and pay-per-use pattern. This pay-per-use pattern based on the resources consumption e.g. processing power, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. In cloud computing the client data is maintained in the data centre of a cloud provider like Tata, Netmagic, Google, Amazon and Microsoft etc. Since the data is stored on Internet Cloud the user will have limited or no control over the data, which may lead to various security issues. Since the data custody is at data centre which could lead to threats such as data leakage, insecure interface, sharing of resources, data availability and inside attacks etc. There are various challenges for adopting cloud computing such as well managed service level agreement (SLA), Confidentiality, Integrity and Availability (CIA). This research paper outlines cloud computing industry models and issues associated with it. This research paper analyse the challenges which are present in cloud computing and best practices by service providers.

KEYWORDS: Cloud Computing, Cloud Security, Challenges and Opportunities, Cloud Service Provider (CSP)

I. INTRODUCTION

In Cloud Computing architecture the computing resources are centralized and scalable and on demand can be offered as services. Like ISPs (Internet Service Providers), the CSPs (Cloud service providers) offer cloud platforms for their customers to create their web services on the internet. Cloud computing enables convenient use and on-demand access to a shared pool computing resources, like servers, storage, applications that can be rapidly provisioned and released with minimal effort. In general CSPs offer three types of services i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). There are various reasons for organizations to move towards IT solutions that include cloud computing as they are just required to pay for the resources on consumption basis [1]. In addition, organizations can easily meet the needs of rapidly changing markets to ensure that they are always on the leading edge for their consumers [2]. Cloud computing has become a business necessity, without managing the infrastructure. The cloud computing idea is in reality by the companies like Microsoft, Amazon, Google, Yahoo! and VMWare. This makes it possible for new startups to enter the market easier, since the cost of the infrastructure has greatly reduced. The clouds companies can rent computing power (virtual machines) or storage space (virtual space) dynamically, according to the needs of their business. This allows developers, managers to concentrate on the business value. With the exploit of this technology, users can access heavy applications via lightweight portable devices such as smart phones, Tabs and PCs. Clouds are the new trend in the evolution of the distributed systems, the predecessor of cloud being the grid. The user does not require any special skill sets to control the infrastructure of clouds; it provides only abstraction. It can be utilized as a service of an Internet with high scalability, higher throughput, quality of service and high computing power. Cloud computing providers deliver common online business applications which are accessed from servers through web browser [2].

II. RELATED WORK

In [1] the author's briefly discuss about the cloud computing technology and its architecture. Further there is a description about the cloud computing security architecture and different levels in it. The author also list and discuss the issues such as SLA's, Cloud data management, access controls etc. The Cloud Computing is an offered service over the Internet by dynamically providing scalable resources. The author also discusses about the economic parameters such as capital expenditure (CapEx) and operational expenditure (OpEx). The paper also focuses on technical security issues arising from the usage of Cloud services [4]. The Cloud computing is current buzzword in the market. Cloud computing is much more than simple internet resource sharing. The author discusses about cloud services delivery models as Infrastructure (IaaS), Platform (PaaS), and Software (SaaS) [5]. The document, a white paper by Di Dialogic Corporation (published in 2010) discuss about benefits and challenges in cloud computing. Dialogic® inCloud9™ is a API developed by Dialogic which helps consumer / customer to overcome challenges [6]. The author briefly discusses about the cloud computing model that provides on demand business and IT services over the Internet. One of the main concerns is its data security as its outsourcing of the business data and application to a third party. Cloud service users need to understand the risk of data breaches in the cloud environment [7]. In [8] the term cloud computing was coined and become popular during year of 2008. Since that the cloud computing business or service is growing, which also brings some Challenges and Opportunities. The paper discusses about Issues and Challenges of Security in SaaS model. In [9] the authors discuss the three questions, where by the adoption of the model, could bring profit and quality enhancement in the organisation. [10] The paper has brief discussion on the “Cloud” computing which is build on decades of research in virtualization, distributed computing, utility computing, and, more recently, networking, web and software services. It implies a service-oriented architecture, reduced information technology overhead for the end-user, great flexibility, reduced total cost of ownership, on-demand services and many other things.

III. Understanding Clouds

The cloud can be grouped into categories,

1. Infrastructure as a Service (IaaS)
2. Application Platform as a Service (PaaS)
3. Software as a Service (Saas)

The IaaS contains physical and virtual resources, such as CPU power, storage etc. (e.g. Amazon Web Services). The PaaS provides software framework or programming environment (e.g. Azure Service Platform, Google App engine). SaaS provides software or applications required by operations group or by business (e.g. Google Apps).

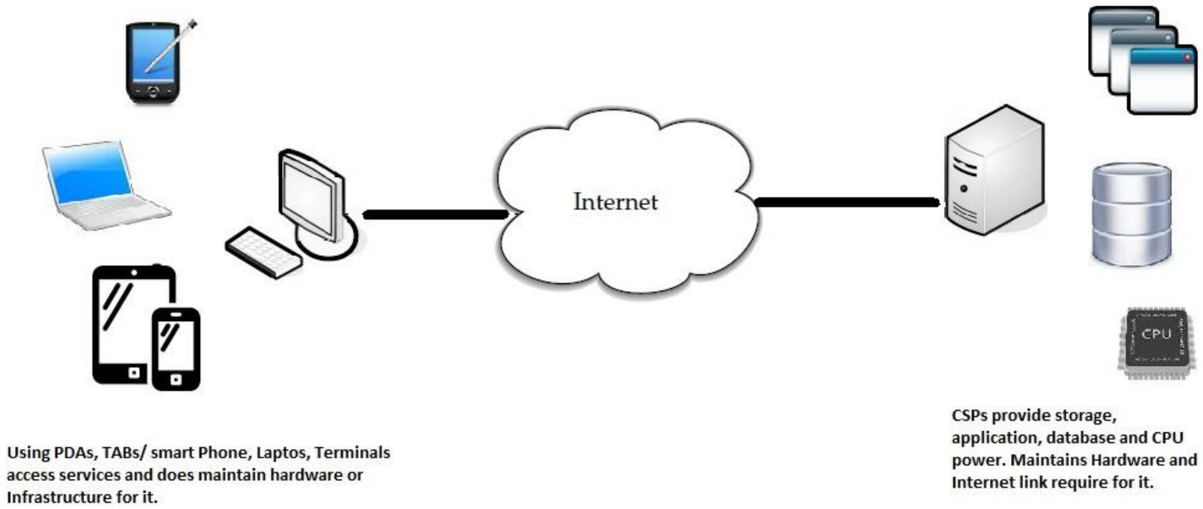
Internet
CPU
Using PDAs, TABs/ smart Phone, Laptos, Terminals access services and does maintain hardware or Infrastructure for it.
CSPs provide storage, application, database and CPU power. Maintains Hardware and Internet link require for it.

Figure 1.0: Cloud computing, companies host your applications.

There are four different cloud deployment models namely Private, Public, Hybrid and Community.

Private cloud: Private cloud may be owned or leased and managed by the organization or a third party and hosted on-campus or off-campus. It is more expensive, but secure compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that might be present in a public cloud environment. In a private cloud, the CSPs and the clients have optimized control over the infrastructure with improved security, as user's access is restricted and networks are known. One of the best examples of a private cloud is Eucalyptus Systems [3].

Public Cloud: A cloud infrastructure is provided to many users, customers and is managed by a third party and exists beyond the organization security perimeter. Multiple organizations can work at the same time on the infrastructure provided and users can dynamically provision resources. These clouds are fully hosted and managed by the cloud provider and fully responsibilities for installation, management, provisioning and maintenance. Customers are only charged for the resources they use, so under-utilization is eliminated. Since consumers have little control over the infrastructure, processes requiring powerful security and regulatory compliance are not always a good fit for public clouds. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used. Public cloud providers such as Google or Amazon offer an access control to their clients. The example of public cloud includes Microsoft Azure, Google App Engine [1].

Hybrid Cloud: It's a combination of two or more of the Private, Public models, where the data is exchanged between them. These clouds would typically be created to segregate responsibilities between the organizations and the cloud service providers (CSPs). In this model, a company can outline the goals and needs of services [4]. A well-constructed hybrid cloud can be useful for providing secure services such as receiving customer payments, as well as those that are secondary to the business, such as employee payroll processing. The major challenge in the hybrid cloud is effective creation and governance of such a solution. The interactions between private and public components can make the implementation even more complicated. In Amazon Web Services (AWS) is an example of Hybrid Cloud where, the private, community or public clouds are linked by a proprietary or standard technology that provides portability of data and applications among them composing clouds.

Community Cloud: This model is rarely offered by CSPs. In this type the Infrastructure is shared by several organizations for a common goal / cause. These clouds are normally based on an agreement between related business organizations such as banking or educational organizations. A cloud environment operating according to this model may exist locally or remotely [1]. An example of a Community Cloud is Facebook.

IV. CLOUD COMPUTING ENTITIES

In Cloud Computing along with providers and consumers there are the two more entities involved in the business i.e. service brokers, resellers and system integrators. These at times they create challenges and issues to the consumer.

Cloud Providers: Includes ISPs (Internet Service Providers), Telecom companies and business process outsourcers that provide either Internet links or data centers (cloud Infrastructure). This enables consumer to access cloud services. Service providers at times involve systems integrators, who build and support the private cloud and offer SaaS, PaaS, IaaS services.

Cloud Service Brokers: Includes IT consultants, business professional service organizations, registered brokers and agents, and influencers that help guide consumers in the selection of cloud computing solutions. Service brokers concentrate on the negotiation of the relationships between consumers and providers without owning or managing the whole Cloud infrastructure. Moreover, they add extra services on top of a Cloud provider's infrastructure to make up the user's Cloud environment [1].

Cloud Resellers: When cloud business expands across continents, the resellers become an important factor. Cloud service providers may choose local IT firms as resellers for their Cloud-based products. Also these cloud resellers create their own products based on infrastructure provided by cloud service providers (CSPs) and offer it to consumers in the region/country.

Cloud Consumers: These are the end users who consume services provided by cloud service providers (CSPs) directly or indirectly through cloud service brokers or resellers.

V. CLOUD SECURITY ARCHITECTURE

Layer	Security Issues
User Layer	Browser / Application: Authentication, SSL, HTTPs implementation, Public-Private Key Implementation
Service Provider Layer	Data Transmission: SLA monitor, Usage accounting and tracking Load Balancer Service (LBS) Policy Management User Identity Infrastructure refresh Audit and Regulatory Compliance etc.
Virtualization Layer	Virtual Machine –Virtual Machines creation, monitoring and operating system software on it. VM allocation to customers / consumers
Data Centre Layer	Physical security: network devices and servers Physical Infrastructure: Servers, CPU's, memory (RAM) and storage Identity and access management Legal and regularity compliance issues,

The Open Security Architecture (OSA) is an organization focusing on cloud security issues.

VI. KEY BENEFITS

Following are some of the benefits offered by cloud computing services and applications:

1. Cost Savings — it is the most cost efficient method to use, maintain and upgrade the IT setup. The software license costs to a company a lot in terms of finances. Adding up of the license fees for multiple users can prove to be very expensive for the organizations. On the cloud, is available at much cheaper rates and hence, can significantly lower the company's IT expenses.
2. Pay as per Use — there are many one-time-payment or pay-as-you-use options available, which makes it very reasonable for the consumer company. The consumer company can demand for more cloud resources when required and can release when they are not in use.
3. IT support cost — requires fewer in-house IT resources to provide system support.
4. Almost Unlimited Storage — Storing information on the cloud gives consumer almost unlimited storage space. Hence, no more need to worry about running out of storage space. (e.g. Google Drive)
5. Scalability / Flexibility — companies can start with a small deployment on cloud and can grow to rapidly, then scale it back if required. Also, the flexibility of cloud computing allows consumer companies to use extra resources as required, enabling them to satisfy their needs.
6. Backup and Recovery — services using multiple redundant backup sites, which can support business continuity and disaster recovery. Since all data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device. Hence, this makes the entire process of backup and recovery much simpler than other traditional methods of data storage.
7. Work from anywhere — the access to the information is from anywhere using Internet connection with proper credentials and access rights. This convenient feature lets user move beyond time zones and geographic location issues.
8. Mobile Accessible — mobile workers have increased productivity due to systems accessible in an infrastructure available from anywhere.
9. Quick Deployment — Cloud computing gives the advantage of quick deployment of desired or required setup. The entire system setup can be fully functional within few minutes, condition the exact kind of technology that user needs is available. Automatic Software Integration is very easy as user / decision maker needs to handpick those services and software applications that are best suit for that organization. Access to information is through APIs that does not require application installations on to PCs.
10. Maintenance — cloud service providers (CSPs) do the system maintenance.

VII. POSSIBLE THREATS AND CHALLENGES

Following are the possible threats and challenges while choosing cloud computing as an option over traditional data centre or server room based option.

1. Technical Issues – Due to some serious malfunction / dysfunction could lead to denial of access to information and data from the cloud anytime and anywhere at all. The fact is that the technology is always prone to outages and other technical issues. Even the cloud service providers (CSPs) run into trouble, in spite of maintaining high standards of maintenance. Besides this, consumer needs a very good Internet connection (broad band link) to be logged onto the server at all times. Consumer might invariably stuck in the case of network and connectivity problems.
2. Hosting (location of data centers) – The resellers, distributors often offers best plans and consumers buy them without thinking of backend cloud data centre location. In case of downtime resellers, distributors do not give rational / reason behind the downtime of service to consumer. Many time physical collocation of data centre information were not passed by CSPs to next level, which leads to denial of service to customer. Since the data lies on the CSPs infrastructure, consumers get worried and do not get clear idea of uptime of the service. In such cases SLAs would be useless. In some cases pretending as CSPs, might have outsourced data centers to some other party.
3. Security in the Cloud – The data / information is being access from the internet the major issue is security. Before adopting cloud technology, consumers should know that it might be surrendering all organization information to a third-party i.e. cloud service provider (CSPs), this could be great risk. Hence, consumer of cloud need to make absolutely sure that it chooses the most reliable service provider, who will keep your information totally secure. The service level agreement (SLA) with non-disclosure agreement (NDA) could be signed by both CSPs and the consumer organization. The data security can be achieved by implementation of encryption techniques, SSL / TLS in data communication, Data Access List, Web application security by Firewall.
4. Prone to Attack – storing information in the cloud could make your organization vulnerable to external hack attacks and threats. As nothing on the Internet is completely secure and hence, there is always the possibility of stealth of sensitive data.
5. Prone to copy – There could be possibility of internal staff might copy data, if enough security perimeter and audit mechanism is not installed at CSPs end.
6. Security and Privacy — Cloud computing is different from the traditional computing model, it utilizes the virtual computing technology. Where the user data may be scattered in various virtual data center rather than stay in the same physical location. Even sometimes across the national borders, at this time, data privacy protection will face the controversy of different legal systems. Attackers might get chance to analyze the critical task depend on the computing task submitted by the users [5].
7. Reliability — Servers farm in the cloud have the same problems such as your own resident servers. The cloud servers pool also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a big difference in the CSP's service model, once you select a particular CSP, you may be locked-in, thus bring a potential business secure risk [5].
8. Lack of Standards — Clouds have documented interfaces (APIs); however, no standards are associated with these APIs, and thus it is unlikely that most clouds will be interoperable. The Open Grid Forum is developing an Open Cloud Computing Interface to resolve this issue and the Open Cloud Consortium (OCC) is working on cloud computing standards and practices. The findings of these groups will need to mature, but it is not known whether they will address the needs of the people deploying the services and the specific interfaces these services need. However, keeping up to date on the latest standards as they evolve will allow them to be leveraged, if applicable [6].
9. Continuously Evolving — User requirements changes as per business demand and also requirements for interfaces, networking and storage. This means a "cloud" has to evolve and not to remain static.
10. Compliance — various countries have regulations towards the storage and use of data on cloud. Consumer organization requires reporting and audit trails, which cloud service providers (CSP) must enable them for

comply with these regulations. Also the data centers maintained by cloud service providers (CSP) are also subject to compliance towards the regulations.

VIII. CONCLUSION

Like every technology, cloud computing has its advantages and disadvantages. While the technology can prove to be a great asset to the consumer organization, it might cause harm if not understood and used properly. Also, we have seen security issues and challenges for cloud computing.

REFERENCES

1. Mr. Rabi Prasad Padhy, Mr. Manas Ranjan Patra, Mr. Suresh Chandra Satapathy; “Cloud Computing: Security Issues and Research Challenges”; IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011.
2. Venkatesh. P, “Cloud Computing Security Issues and Challenges”, International Journal of Computer Science and Information Technology Research, Vol. 2, Issue 3, pp: (122-128), Month: July - September 2014.
3. Neeraj Shrivastava and Rahul Yadav, “A Review of Cloud Computing Security Issues”, International Journal of Engineering and Innovative Technology (IJEIT), Volume 3, Issue 1, July 2013.
4. Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, “On technical Security Issues in Cloud Computing,” Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.
5. Pankaj Arora, Rubal Chaudhry Wadhawan, Er. Satinder Pal Ahuja; “Cloud Computing Security Issues in Infrastructure as a Service”; International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012 ISSN: 2277 128X.
6. Dialogic (white paper); “Introduction to cloud computing”, 2010.
7. Balasubramanian V. and Mala T.; “A REVIEW ON VARIOUS DATA SECURITY ISSUES IN CLOUD COMPUTING ENVIRONMENT AND ITS SOLUTIONS”; ARPN Journal of Engineering and Applied Sciences; VOL. 10, NO. 2, FEBRUARY 2015.
8. Prof. Divyakant Meva, Dr. C. K. Kumbharana; ” Issues and Challenges of Security in Cloud Computing Environment”; International Journal of Advanced Networking Applications (IJANA) ISSN No. : 0975-0290.
9. Vidyanand Choudhary and Joseph Vithayathil, “The Impact of Cloud Computing: Should the IT Department Be Organized as a Cost Center or a Profit Center?”, Journal of Management Information Systems / Fall 2013, Vol. 30, No. 2, pp. 67–100., ISSN 0742–1222 (print) / ISSN 1557–928X (online)
10. Mladen A. Vouk, Cloud Computing – Issues, Research and Implementations, Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246, doi:10.2498/cit.1001391.

BIOGRAPHY

Sandeep Madhusudan Kelkar is a Assistant Professor in the Information Technology Department of Prin. L. N. Welingkar Institute of Management Development and Research, Mumbai, India (Affiliated with University of Mumbai). He received Master of Computer Application (MCA) degree in 2003 from IGNOU, New Delhi, India. He is perusing Ph. D. from University of Mumbai on the impact of online learning technology. His research interests are Computer data networks, Management Information Systems, Open Source web technologies etc.