IJRSET 2015 SPL Volume 2, Issue 10 Pages: 6-13

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

Cloud Computing Models and itijs Benefits

[1] **P.Samundeeswari, Msc., (M.Phil),**
[1] Assistant Professor,
[1] Department of Computer Science,
[1] Dr.N.G.P Arts and Science College.

Abstract:-

We decided to focus on the categorization of cloud benefits by looking at the deployment and service modelsused to describe cloud computing. Researching the services and models are available is hard to do because cloudcomputing offerings are emerging at a rapid pace. It is notonly hard to keep track of all the cloud computing offerings,he cloud computing paradigm itself is also rapidly evolving.Finding out which services are offered and deriving which model are used for each of these services, is animpossible goal to achieve in a market this big and developingthis fast. As a result, creating a mapping of which securitycontrols are implemented by each cloud provider is a goalaimed too high as well.

What is cloud computing?

Cloud computing is defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Cloud computing is comparable to grid computing, a type of computing where unused processing cycles of all computers in a network are harnesses to solve problems too intensive for any stand-alone machine. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services such as servers, storage and applications are delivered to an organization's computers and devices through the Internet.

Figure 1: Cloud Model

Cloud providers: Major corporations including Amazon, Google, IBM, Sun, Cisco, Dell, HP, Intel, Novell, and Oracle have invested in cloud computing and offer individuals and businesses a range of cloud-based solutions.

Social Networking: Perhaps the most famous use of cloud computing, which does not strike people as "cloud computing" at first glance is social networking Websites, including Facebook, LinkedIn, MySpace, Twitter, and many, many others. The main idea of social networking is to find people you already know or people you would like

to know and share your information with them. Of course, when you share your information with these people, you're also sharing it with the people who run the service.

E-Mail: Some of the biggest cloud computing services are Web-based e-mail. As of January 2009, over 500 million people used Microsoft's Web-based e-mail, Hotmail or Windows Live Mail. Using a cloud computing e-mail solution allows the mechanics of hosting an e-mail server and maintaining it to be taken out of your hands. It also means that your e-mail is accessible from anywhere.

Document/Spreadsheet/Other Hosting Services: As made famous by Google Docs, a number of services like Zoho Office exist on the Internet that allow you to keep and edit your documents online. By doing so, the documents will be accessible anywhere, and you can share the documents and collaborate on them. Multiple people can work in the same document simultaneously.

Backup Services: Even if you do use services to keep all your documents and photos, chances are you still have data on your personal computer. One of the biggest problems with personal computing has been the tendency to lose that data if your computer is stolen, destroyed, or the storage device damaged. This is where backup comes in. Sometimes, even backing up to media you have isn't good enough -- you need to store the data off-site for more complete protection. Services like JungleDisk, Carbonite, and Mozy allow you to automatically back up all your data to servers spread around the country or world for a surprisingly low price. Of course, your data is then susceptible to security breaches. Similarly, services like Simplicity and Drop box (both offer free versions) make it easy to keep local copies of files on multiple computers synchronized while keeping a copy in the "cloud." Some of these services will even keep previous versions of files or deleted files in case you happen to delete or mess up an important file.

Banking and Financial Services: Consumers store personal financial information to cloud computing service providers. In addition, consumers store tax records using free or low cost online backup services.

Health Care: In an effort to improve the nation’s health IT infrastructure, the Department of Health and Human Services’ (HHS) Office of the National Coordinator for Health Information Technology (ONC) recently selected a cloud computing platform to manage the selection and implementation of Electronic Health Record (EHR) systems across the country.Non-health care organizations as Google and Microsoft provide a means by which consumers can create an online personal health record (“PHR”). Google Health and Microsoft HealthVault allow the public to create, store, and access online personal health records on the search engine's website.

Government: Apps.gov - In October 2009, the U.S. government launched “Apps.gov”, a website providing cloud-based computing services for federal agencies. The decision was largely motivated by the desire to reap the cost savings.

Local Government: The Los Angeles City Council: In October 2009, the city council agreed to shift the city’s email system was shifted to Google’s Gmail cloud computer platform. The Los Angeles Council and Google agreed that the data stored for the city belongs to the city, and Google will notify the city of all requests for data and security breaches so the city can take actions it deems appropriate.

Cloud computing - an irreversible trend:

Cloud computing in its various forms:

Cloud computing allows smart use of the potential offered by the Internet. Both businesses and public authorities view it as a useful and unstoppable development in information and communication technology (ICT), which modernizes and improves services and operational management. Implementations will succeed only if data, data security and data traffic via the Internet are handled in a careful and well-managed way from day one. Cloud computing differs conceptually from existing ICT arrangements. A key difference is that users do not have to store information on data carriers such as PCs and USB sticks. That is a major advantage. Surveys reveal that business-sensitive information is held insecurely on hard drives in over 60 percent of workstations and laptops. The best known are social media. Social apps (cloud-based applications)such as Hyves, LinkedIn, and Face-book are used daily by millions of people around the world. Users now store data not on their own PC but somewhere in the cloud. Another example is the increasing use of thin-client computers. These are computers with very limited storage and processing capacity. They provide access to applications and remote storage via a (web) browser. A thin client is, therefore, nothing more than an information viewer that seeks to connect to the World Wide Web. You read your email, download videos or use word-processing applications directly on the Internet.

What are the benefits of cloud computing?

Cloud solutions offer innumerable benefits:

Joined-up government: Government services are increasingly being provided via the Internet, which acts as a virtualized counter for public services. In this way public authorities can be contacted seven days a week, 24 hours a day. Citizens and businesses increasingly expect that. They are also less concerned about the way in which authorities organize themselves be-hind the computer screen. Whether for a tax return, a licence or benefit application, the customer expects the authority to know who he is and link up the relevant files, there-by keeping the number of trans-actions to a minimum. This is all possible using the cloud as the basic framework. After all the government services have been interlinked, the next step in the modernization of service provision is the enrichment of the available information via social media, and communication via social media by public authorities, citizens, and businesses.

Lower costs/less ICT investment in the workplace: Unwieldy computers under or on desks will be replaced by a tiny box that manages traffic via the Internet. The benefits are lower costs in the investment and opera-tional phases for hardware, and licences which are no longer required in the workplace but which can be accessed via the cloud. Also fewer ICT personnel are required on the shop floor to keep computers running. The savings on workplace facilities alone are considerable. For example, the US Federal Government is aiming to achieve savings of more than 60 percent on licence costs for the use of email (source: CIO.gov). The range of tried-and-tested applications and services available in the cloud is growing daily, including for the support of operational management functions (personnel, information, organization, finance, computerization, communication, and accommodation). This substantially reduces the time required to implement new ICT systems. They are no longer built or purchased, but are selected and paid for on a per-use basis on the Internet.

Consistent supplier management: The introduction of cloud computing enables us to purchase and use ICT resources in a more

coordinated and consistent manner. ICT decisions are currently taken across multiple levels and departments within governments. The relationship with business is changing. Public authorities can greatly reduce the number of commercial relationships by signing contracts with partners on the basis of a one-stop-shop model.

What cloud services are available on the market?

Figure 1 identifies the main security services in the different layers of cloud environments. These services and their operation within the cloud environment are described below.

Data encryption services: Most people believe that the cloud services in the market provide a lower level of security than their own data center. The question is whether this is an accurate observation. In many cases the cloud service provider will have a higher level of security than most data centers and outsourcing providers. There are two possible reasons for this. First, cloud service providers take a standardized, general approach to security. Moreover, they simply cannot afford to lose customers as a result of deficient security. A single newspaper report about a serious data leak could mean the end of a cloud provider, particularly if it involves data that government institutions are legally required to keep under surveillance. Cloud providers are therefore focused on information security from day one. It is their most important priority. How do you know your provider has implemented the right level of security measures? If there is insufficient control of the system in which the data is stored, it is necessary to ensure that the security of the data itself is controlled. By using data encryption and retaining control of encryption key management, organizations can take full advantage of cloud computing.

Authorization management services: Authorization management services ensure that the right user accounts with the right information are available in the relevant systems. If that is not properly implemented, access control will be a mere illusion. All accounts, including administrative accounts, must always be related to individuals in order to prevent abuse. The first step is, therefore, to manage the entire life cycle of accounts related to individuals (employees, partners, customers, etc.). This must include the functional accounts (for example, administrators) that are linked to these identities at any given time. Identity and authorization management is liable to be a complex matter within the organization.
Outside the boundaries of the organization, however, such as in ecosystems, supply-chain channels or cloud services, identity and authorization management is essential for operational management. Applications can be moved to the cloud, but control of authorizations must remain within the client organization. This does not mean, however, that the actual identity and authorization management cannot be carried out in the cloud; on the contrary, Identity-as-a-Service can be very useful in the outsourcing of identity management and the facilitation of a model such as e-Recognition as implemented in the Netherlands, which enables users to log into various government institutions through their own account. Always be aware that combining cloud services and cloud security services in the same cloud will only be effective if the cloud service provider can effectively guarantee functional separation.

Access control services: Authorization management may then be a requirement, but if access control measures fail to operate effectively, your data will be unprotected without your being aware of it. If the access control is too tight, however, operational management may be impeded. Access control measures must ensure a balance

between practicability and security, and must be based on the relevant risks. Another important aspect is the integration of access control measures in your data center, your outsourcing partner's data center and the cloud applications used. Single sign-on (SSO) across the boundaries of the organization and relationships of trust between organizations are essential for the successful use of cloud services.

Cloud integration services: People generally speak of "the" cloud. However, it is unlikely that there will be a single cloud containing all the organization's applications. Some office applications may be obtained from Google, for example, whereas the CRM is with Salesforce.com. The security services may in turn be supplied by a dedicated security provider. This not only means that all employees must have access to all these services from any location, but also that cloud services must have access to each other's network for specific services. Consideration must also be given to where brokers and other generic ICT services will be accommodated, such as the enterprise service bus (**ESB**) or print servers. At present, we appear to be creating the same islands or 'stove pipes' that we have been trying to get away from in our own data centers in the last ten years. All these services must be integrated in a secure and controllable way. The cloud services must communicate with standard protocols for web services in order to achieve genuinely secure cloud integration.

Communication security services: Cloud services - and hence data be-longing to citizens and businesses - may be located anywhere and transmitted frequently via the Internet. During transmission, the data must be secured by standard protocols. Encryption is also an option, but it is too complex to store all data in encrypted form. It will probably only be necessary to store business- or privacy-sensitive data in encrypted form. The rest must nevertheless be protected during transmission via the Internet. This can be achieved by means of standard protocols such as SSL/TLS. Network traffic can be protected by PKI based protocols. Even more important than traffic to end-users is traffic between service providers. This must also be encrypted, but you will probably not own the keys used, which means you will incur a risk when services of different service providers are integrated.

Business continuity service: Business continuity management (BCM) is an important area of attention for all government organizations. The drawing up of detailed emergency plans for unforeseen disasters, such as denial-of-service attacks on government websites, is essential nowadays. In the ICT sector, that means backups of business critical data must be available at different locations. Cloud service providers such as Google, Microsoft, and Amazon are very useful in this regard. They promise 99.9 percent uptime and their services release organizations from the burden of creating and maintaining a backup

Monitoring and auditing services: If security levels are not being measured, it will be difficult to assess the status and quality of these security levels. It is important to have access to monitoring and auditing services, either in-house or with a cloud service provider, where all the information from the client data center, the outsourcing provider, and the cloud services provider will be gathered for further processing. This solution must be able to receive log files from all systems in order to process security warnings from all systems.
This is a labor-intensive process requiring people with very specific skills to analyse the results. It is, therefore, advisable to also use this service in the cloud, with all other cloud and non-cloud services being connected.

infrastructure and recovery facilities. BCM incorporates various complementary elements, such as disaster recovery, business recovery, business resumption, contingency planning, and crisis management. However, disaster recovery alone is not sufficient.

Cloud computing in its various forms: Cloud computing is an important trend in the field of information provision and related ICT. It turns computer processing power and data storage into a utility for collective use, as has long been the case of gas, water, and electricity. The rise of cloud computing has been particularly strong, is set to continue, and is irreversible. In view of the advantages for government organizations, cloud computing should also be trusted and supported within the public sector, both at central and local government levels and within executive agencies. The actions required in order to mi-grate securely and carefully to the cloud can be summarized as follows:

1. Formulating a clear security policy including security requirements;
2.Organizing the management among the government organizations and market participants concerned;
3. Acquiring the required expertise in the field of cloud computing and demand management;
4. International coordination for the exchange of knowledge and experience.

- It is important that all government institutions cooperate consistently with each other. Security requirements must be supported by all government institutions. Otherwise all the benefits will be negated and, chaos will result. Overall management of the formulation and implementation of the security policy must be guaranteed.
- The public services provided by the government, with ICT as an enabler, extend beyond the boundaries of ministries and local governments. This applies particularly to the use of applications offered by cloud computing.
- The authority to decide on and implement cloud computing models must therefore cut across departmental boundaries. Cloud computing is too complex and too generic to assess risks, develop security concepts, and select services individually in each government body. The security requirements should be translated into a clear SLA. and additional measures.
- Cooperation is important. The chal-lenges involved in adopting cloud services, and the scale of the potential risks and benefits demand that risk assessments, security frameworks and service selections be elaborated on a pan-governmental basis.
- Governments must also align their security and privacy policy regulations to the new reality, coordinate them effectively with those of the other EU member states, and test them against those of non-EU states. That will prevent unauthorized reading of data and breaches of privacy rules

Types of Cloud Computing: Cloud computing is providing developers and IT departments with the ability to focus on what matters most and avoid undifferentiated work like procurement, maintenance, and capacity planning. As cloud computing has grown in popularity, several different models and deployment strategies have emerged to help meet specific needs of different users. Each type of cloud service, and deployment method, provides you with different levels of control, flexibility, and management. Understanding the differences between Infrastructure as a Service, Platform as a Service, and Software as a Service, as well as what deployment strategies you can use, can help you decide what set of services is right for your needs.

Cloud Computing Models: There are three main models for cloud computing. Each model represents a different part of the cloud computing stack.

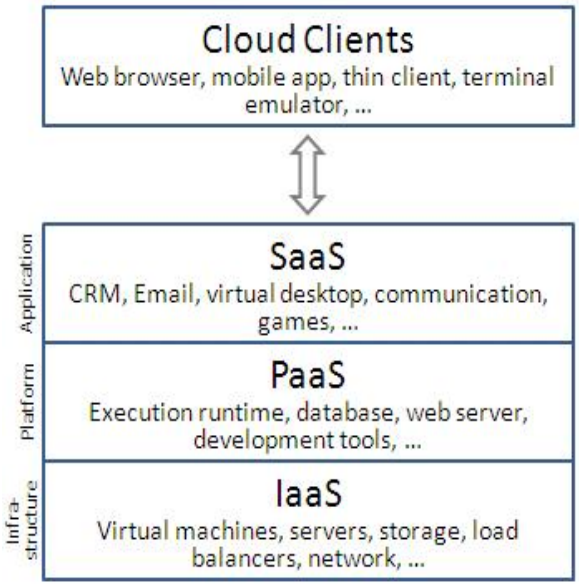

Figure 2: Cloud Architecture

I. Infrastructure as a Service (IaaS): Infrastructure as a Service, sometimes abbreviated as IaaS, contains the basic building blocks for cloud IT and typically provide access to networking features, computers (virtual or on dedicated hardware), and data storage space. Infrastructure as a Service provides you with the highest level of flexibility and management control over your IT resources and is most similar to existing IT resources that many IT departments and developers are familiar with today.

II. Platform as a Service (PaaS): Platforms as a service remove the need for organizations to manage the underlying infrastructure (usually hardware and operating systems) and allow you to focus on the deployment and management of your applications. This helps you be more efficient as you don't need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running your application.

III. Software as a Service (SaaS): Software as a Service provides you with a completed product that is run and managed by the service provider. In most cases, people referring to Software as a Service are referring to end-user applications. With a SaaS offering you do not have to think about how the service is maintained or how the underlying infrastructure is managed; you only need to think about how you will use that particular piece software. A common example of a SaaS application is web-based email where you can send and receive email without having to manage feature additions to the email product or maintaining the servers and operating systems that the email program is running on.

CONCLUSION

There are many more players in the on-demand market that many reports acknowledge. These range from basic infrastructure offerings (IaaS), through platform support (PaaS) to full applications (SaaS).The long term cost of ownership may at first not seem to add up, but take into consideration other factors such as reduced risk and added value and for many organizations on-demand services make a lot of sense.

REFERENCES

[1] Gens, F.: IT Cloud Services User Survey, part 2: Top Benefits and Challenges(2008)

[2] John D.Sutter, Twitter Hack Raises Questions About "Cloud Computing," CNN, July16,2009,http://www.cnn.com/2009/TECH/07/16/twitter.hack/index.html.

[3] Amazon. Amazon Elastic Compute Cloud(EC2),2010/http://www.amazon.com/ec2/S [accessed: 10December2009].

[4]BernardGolden.Definingprivateclouds,2009/http://www.cio.com/article/492695/Defining_Private_Clouds_Part_OneS [accessed on:11January2010].

[5]Boss,MalladiP,QuanD,LegregniL,HallH. Cloudcomputing,2009,p.4http://www.ibm.com/developerswork/websphere/zones/hipods/library.htmlS [accessedon:18October2009].

[6] Michael Miller, "Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online", August 2008
[7] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing," 2009, http://www.wheresmyserver.co.nz/storage/ media/faq-files/clouddef-v15.pdf, Accessed April 2010.
[8] Frank Gens, Robert P Mahowald and Richard L Villars.(2009),IDC Cloud Computing 2010.
[9]http://sushilresearch.wordpress.com/2013 /05/04/cloud-computing
[10] Jason Bloomberg, “Data Remanence: Cloud Computing Shell Game,” May 19, 2011.http://www.zapthink.com/2011/05/19 dataremanence-cloud-computing-shell game/.
[11] Amazon EC2 goes down, taking with it Reditt, Four Square and Quora. http://eu.techcrunch.com/2011/04/21/amazo n-ec2-goesdown-taking-with-it-reddit foursquare-and-quora/.