Cloud Revolution in Government

[1]Snehal Kambale and [2]Gaurav Walia
[1]National Informatics Centre, Mumbai, India
snehal.k@nic.in
[2]National Informatics Centre, New Delhi, India
gaurav.walia@nic.in

Abstract—**Cloud computing involves deploying sets of remote servers and software networks that allow centralized data storage and internet based having access to computer services or resources. Government has decided to adopt cloud computing and delivering computing resources to users. G-cloud is the public sector service for the secure cloud computing with efficiency, standardization, sharing and reuse of resources. In this paper we will see infrastructure of cloud along with benefits, opportunities and challenges of cloud in Government sectors.**

Index Terms— **Cloud computing, Governance, G-cloud, Security issues.**

I. INTRODUCTION

Cloud computing is a new technology in Information technology which plays main role in economic growth as it connects people to data, information and computing services anywhere and anytime. Services to citizens such as Governance, banking, insurance, healthcare, agriculture, transport, education, scientific investigations, healthcare, supply chain management, business, commerce and finance organizations and many more are increasingly moving to the cloud, mainly because it is cheaper, had infinite storage capacities and mobility. While the private sector is building various benefits on cloud computing, significant part of the global development of cloud computing technologies and solutions is also happening in Government sector. The Cloud Computing Innovation is an open platform aimed at bringing together subject matter experts across Government, industry, and academic to collaborate and innovate with the objective of accelerating the emergence of the Government IT ecosystem as a strong global leader in Cloud Computing technologies. Even though many facilities are provided by cloud computing, there are some challenges on use of cloud computing with respect to security, service quality, interoperability, legal matters and privacy.

II. KEY CONCEPT AND TECHNOLOGY

A. Objectives of Cloud Computing

- Optimum utilization of infrastructure.
- An illusion of the availability of infinite computer resources on demand
- Speeding up the development and deployment of applications.
- Easy replication of successful applications to avoid duplication of effort and cost in development of similar applications.

- Availability of certified applications following common standards at one place.
- Data recovery and application continuity through disaster recovery facility.

Cloud computing refers to both the applications delivered as services over the Internet and the hardware/ software in the data centers that provide services. There are four basic cloud delivery models, based on who provides the cloud services. These four delivery models are:

1. *Public clouds* are provided by a designated service provider and may offer either a dedicated or shared operating environment with all the benefits and functionality of elasticity and the accountability/utility model of cloud. One of the advantages of a public cloud is that they may be larger than an enterprise cloud, and hence they provide the ability to scale as on demand.

2. *Private cloud* in which cloud services are provided solely for an organization and are managed by the organization or a third party. These services may exist off-site.

3. *Community cloud* in which cloud services are shared by several organizations for supporting a specific community that has shared concerns (e.g., mission, security requirements, policy). These services may be managed by the organizations or a third party and may exist offsite.
   A special case of community cloud is the Government or **G-Cloud**. This type of cloud computing is provided by one or more agencies (service provider role), for use by all.

4. Hybrid cloud which is a composition of different cloud computing infrastructure (public, private or community). An example for hybrid cloud is the data stored in private cloud of a travel agency that is manipulated by a program running in the public cloud.

III. ARCHITECTURE

A. Cloud Service Delivery Models

Based on architecture, four individual models are:

Software as a Service (SaaS): In this model**, t**he capability provided to the organization is to use the provider's applications running on a cloud infrastructure and accessible from various client devices through any web browser. It means a complete application is offered to the organization as a service on demand. On the organization side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted and maintained. Organization do not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited organization specific application configuration settings. Thus, benefits of using SaaS are easier software administration, automatic updates and patch management, software compatibility across the business, easier collaboration, and global accessibility.

Platform as a Service (PaaS): In this model, a layer of software or development environment is encapsulated and offered as a service, upon which other higher levels of service are built. The organization has the freedom to build his own applications, which run on the provider's infrastructure. Hence, a capability is provided to the organization to deploy onto the cloud infrastructure organization -created applications using programming languages and tools supported by the provider (e.g., Java, Python, .Net, .Asp etc.). Although the organization does not manage or control the underlying cloud infrastructure, network, servers, operating systems, or storage, but organization has the control over the deployed applications and over the application hosting environment configurations.

Infrastructure as a Service (IaaS): This model provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data center space etc. are pooled and made available to handle workloads. The capability provided to the organization is to storage, networks, and other fundamental computing resources where the organization is able to deploy and run software, which can include operating systems and applications. The organization does not manage or control the underlying cloud infrastructure but has the control over operating systems, storage, deployed applications, and possibly select networking components (e.g. firewalls, load balancers etc.).

Storage as a Service (STaaS): This model provides need based storage solution. It provides excellent alternative to the traditional on-site and dedicated storage systems and reduces the complexities of deploying and managing multiple storage tiers. It can be used to mitigate risks in disaster recovery, provide long-term retention for records and enhance both continuity and availability.

IV. E-GOVERNANCE

Cloud computing significantly speed up design and roll out of services, enable social networking and participative governance and e-Commerce on a scale which was not possible with traditional technology solutions. So Government has decided to adopt cloud computing to address issues typically faced by different departments at the state, such as long IT infrastructure procurement cycles, under utilization of resources, need for dynamic scalability, appropriate disaster recovery of applications and data, simplifying IT infrastructure provisioning and availability to departments. After having analyzed infrastructure at the present provisioned and technology advancements Government has initiated the process of implementing cloud based services to different Government organizations, citizens and businesses. By adopting cloud computing, the Government able to more easily exploits and share commodity of information and communication technology products and services. The vision for Government is to support a public cloud solution. In addition to accelerating the delivery of e-services to citizens and businesses, the Government's cloud-based service delivery platform also support a number of other objectives including increased standardization, interoperability and integration and under-utilized resources. Previously Government organizations has used moderate to low level of IT involvement , still the greatest value gained by changing the way we operate on cloud system. Still there are some challenges with G-cloud to overcome traditional technology like lack of common policies for application reuse, individual technology along with lack of infrastructure standardization.

A. Advantages of cloud in Government

1   Rapid deployment of application: Currently, Deployment of any Government project requires long cycle of procurement of infrastructure, application development and testing. G- Cloud environment provides the requisite platform for faster deployment of applications as infrastructure and platform can be procured as service. This essentially saves overall time required for development and deployment of applications.
2   Common set of protocols, guidelines and standards for G-Cloud.
3   Optimum utilization of existing infrastructure: Governance related required information can be shared among Government bodies using G-cloud. So duplication of services can be avoided and efficiency level can be increased when cloud is used for such sharing.
4   Efficient service delivery: Improve quality of content along with standardizing the content and delivery of application.
5   Reduced cost: As information is maintained in common virtual cloud, organization can access information from different location and maintaining data along different agencies can be avoided.
6   Data availability: Different kind of data within Government organizations can be easily available.
7   Improvement in inter-organizational co-ordination. Thus, improvement in administrative efficiency, productivity and citizen services can be achieved.

B. Risks and Issues in G-Cloud Computing

- *Multi-tenancy:* Multi-tenancy refers to sharing physical devices and virtualized resources between multiple independent organizations. Attacker could be on the same physical machine as the target. G-Cloud use multi-tenancy features to build infrastructures however the sharing of resources means that it can be easier for an attacker to gain access to the target's data.
- *Loss of Control:* Loss of control is another potential breach of security that can occur where organizations's data, applications, and resources are hosted at the G- cloud. As the organization do not have explicit control over their data, this makes it possible for G-cloud providers to perform data mining over the organization's data, which can lead to security issues. In addition, when the cloud providers backup data at different data centres, the organization cannot be sure that their data is completely erased everywhere when they delete their data. This has the potential to lead to misuse of the unerased data.
  In these types of situations where the organizations lose control over their data, they see the cloud provider as a black-box where they cannot directly monitor the resources transparently.
- *Trust Chain in Clouds:* Due to loss of control, organization rely on the cloud providers using trust mechanisms as an alternative to giving organization's transparent control over their data and cloud resources. Therefore cloud providers build confidence amongst organizations by assuring them that the provider's operations are certified in compliance with organizational safeguards and standards.

- *Access:* The access privilege for data must be provided only to the authorised users of organization and auditors in order to minimize such risks. When there is an access from an internal to external source, the possibility of risk is more in case of sensitive data. Segregation of the data is very important in cloud computing as the data is distributed over a network of physical devices. Data Corruption arises if appropriate segregation is not maintained.
- *Network Load:* Cloud network load can also prove to be detrimental to performance of the cloud computing system. The computers and the servers crash due to high volume motion of data between the disk and the computer memory. Flexibility and scalability should be considered when designing and implementing a cloud infrastructure. Money and time also plays an important role in the design of the infrastructure. Organizations always have expectations on the durability and the efficiency of the system.
- *Data Security:* Data has to be appropriately secured from the outside world. This is necessary to ensure that data is protected and is less prone to corruption. Encryption is the one keytool is used by organization to protect data.
- *Data Location:* Data Location is another aspect in cloud computing where service providers are not concentrated in a single location but are distributed throughout the globe. It creates unawareness among the users about the exact location of the cloud. The users may not be familiar with the varied components in the cloud.

V. CONCLUSION

The cloud model ultimately serve to transform - in a big way - not just IT in the corporate world but government information technology, as well. Cloud provides lots of opportunities to different departments of government which leads to revolution in Government. However, it will require careful development of a national Cloud strategy to ensure that maximum benefits of the Cloud can be provided to the nation while minimizing the risks.

REFERENCES

[1] Security and Privacy Issues in Cloud Computing, Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA, 2014
[2] IBM Blue Cloud Initiative Advances Enterprise Cloud Computing. http://www.03.ibm.com/press/us/en/pressrelease/26642.wss. (Accessed on: November 20, 2012).
[3] GI cloud computing strategic report, DeitY, 2013
[4] Chapter 1 Cloud Computing: Reviews, Surveys, Tools, Techniques and Applications – An Open-Access eBook by HCTL Open http://ebooks.hctl.org ISBN-13 (PDF): 978-1-62951-802-2
[5] Cong Wang, Qian Wang, KuiRen, and Wenjing Lou, Ensuring Data Storage Security in Cloud Computing, 17th International workshop on Quality of Service, USA, pp.1-9, ISBN: 978-1-4244-3875-4, 2009
[6] D.C. Wyld, Moving to the cloud: An introduction to cloud computing in government. Washington, DC: IBM Center for the Business of Government, November 2009
[7] ICT-System-Assurance, Cloud Computing Information Security and Privacy, 2014
[8] Security guidance for critical areas of Focus in cloud computing, 2014.
[9] C. Johnson, "CIO technology survey results," CIO, October 1, 2009. http://www.cio.com/article/503874/CIO_Technology_Survey_Results
[10] ITPP in association with HP," Government cloud computing adoption,
     " http://www.itproportal.com/2014/07/21/government-cloud-computing-adoption/, 2014
[11] Volume 3, Issue 1, ISSN: 2327782 (Online), International journal of research in computer sciences and management studies, 2015
[12] T.P. Strecker, "Govt IT procurement in for shake-up," The Dominion Post, June 22, 2009. [Online]. http://www.stuff.co.nz/technology/2521317/Govt-IT-procurement-in-forshake-up [Accessed: September 11, 2009].
[13] http://www.cisco.com/c/dam/en_us/about/ac79/docs/sp/Cloud_Computing.pdf, 2009