ISSN:0975-9646

Review on Benefits and Security Challenges of Cloud Computing

Nasarul Islam.K.V

Abstract — **Cloud computing is fastest booming technology; nowadays it has remarkable position in business concern. This technology has changed the face of traditional computing technologies, it is the simplest service available through internet to start and maintain business. Facilities of this technology are available through internet by paying amount based upon demand in an easier and efficient manner with the functionality of increase or reduce the requirements. This technology has numerous advantages, even though it has not satisfied its maturity level due to the lack of security and other issues. This paper deals with the various advantages and security challenges of cloud computing. It also point out the various service models of cloud computing.**

Keywords— **Cloud computing, Benefits, Security challenges, Service Models, Review.**

I. Introduction

Cloud computing is fastest growing technology, easiest service available computation technology for business organizations through internet. It can serve many facilities to business organizations such as resources, infrastructure, etc by paying amount on demand basis over network with functionality of increase or reduce requirements. It has capacity to meet any IT industrial requirements. It provides users to store, manage and create their applications on cloud, also provides virtualized resources in dynamically, bandwidth and other services. It helps users to overcome economical and technical barriers while starting an organization. It also helps to start organizations in temporarily mode without huge investment, slowly watching the performance of organization, can take decision to increase or reduce requirements. Irrespective of size of organization such as small, medium or large, it is useful to all type of enterprises. These facilities changed the face of computing.

As discussed above, it offers many services than traditional IT models but from the consumer prospective, cloud computing security concerns remain a major problem for its adoption [3]. Data or information is important nowadays, its values are uncountable. Keeping this information in an open network is automatically creating doubt on the secrecy, availability, misuse of information. According to a survey carried out by Gartner [7], more than 70% of Chief Technical Officers believed that the primary reason for not using cloud computing services is that of the data security and privacy concerns.

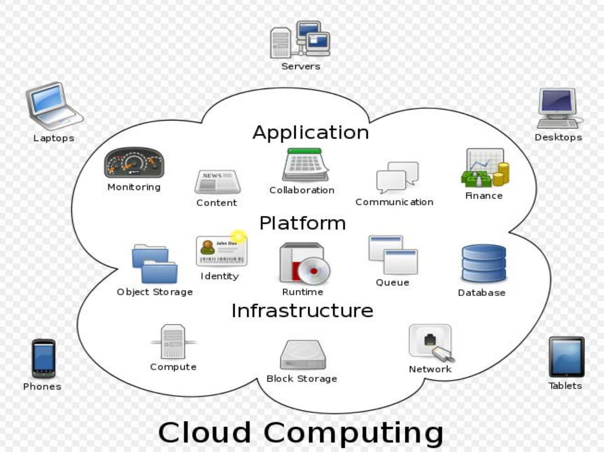


Fig.1 Cloud Architecture

II. Cloud Analysis

2.1 DEFINITION OF CLOUD COMPUTING

Definition of cloud computing is “it is a significant distributed computing model that is directed by financial prudence of balance, in which stake of isolate, fundamental, loading, podium in which a facilities are supplied as per the request of exterior foreign clients through the internet”[1]. Various cloud service providers are Amazon, Google, IBM, Microsoft, and Salesforce.com.

2.2 SERVICE MODELS

The services offered by cloud computing can be mainly classified into three. Three service models are explained below.

1, Infrastructure as a Service (IaaS): This is one of key service provided by cloud. It offers various hardware resources in the form of service such as CPU, Memory, Network devices etc. Instead of owning the infrastructure, it can be utilised by lease or rent according to the user's demand. Virtualization is extensively used in IaaS cloud in order to integrate/decompose physical resources in an ad-hoc manner to meet growing or shrinking resource demand from cloud consumers [5].Users can decide CPU usage, size of memory, bandwidth etc, rather than setting up an expensive servers, data centers, etc. This service provides relaxation to the users by not bothering infrastructure, reducing high investment at the beginning of organization. Hardware part is fully controlled by service provider, consumers do not have any control over infrastructure but user can manage and control the softwares and other applications. Amazon EC2 or vCloud are examples of IaaS.

2, Platform as a Service(PaaS): PaaS is a development platform supporting the full "Software Lifecycle" which allows cloud consumers to develop cloud services and applications (e.g. SaaS) directly on the PaaS cloud[6], it provide all services for developing, modifying, testing and running applications in cloud environment, helps to use platform(C, C++, .NET etc)without buying softwares. It provides facility to use platform for multiple users to run same applications at a time. The PaaS model enables resources to be increased easily with demand since end users share the same cloud. This is often called multi-tenant cloud computing [8]. PaaS requires special attention for development environment, configuration management, various tools for development etc. It provide additional tools for development are database, web server etc. User does not have any control over the OS, Server but user can possibly manage the deployed application and its configuration. Azure, Google App engine are examples of IaaS.

3, Software as a Service (SaaS): It provides facility to run various software applications through Internet without installing these in client site. This avoids installing required softwares in individual site and saving purchase amount of these softwares. Cloud users do not have any control over cloud infrastructure, that often employs multi-tenancy system architecture, namely, different cloud consumers' applications are organized in a single logical environment in the SaaS cloud to achieve economies of scale and optimization in terms of speed, security, availability, disaster recovery and maintenance [5]. Service provider controls entire infrastructure such as servers, softwares, etc and provide facility to use applications to consumers and possibly application configuration settings. In SaaS, there is Divided Cloud and Convergence coherence mechanism whereby every data item has either the “Read Lock” or “Write Lock”[11]. SaaS typically involves a monthly or annual fee per user so price is scalable and adjustable if users are added or removed at any point[3]. Some examples of SaaS include - Google Apps, Microsoft office 365, GT Nexus, Marketo and Trade Card.

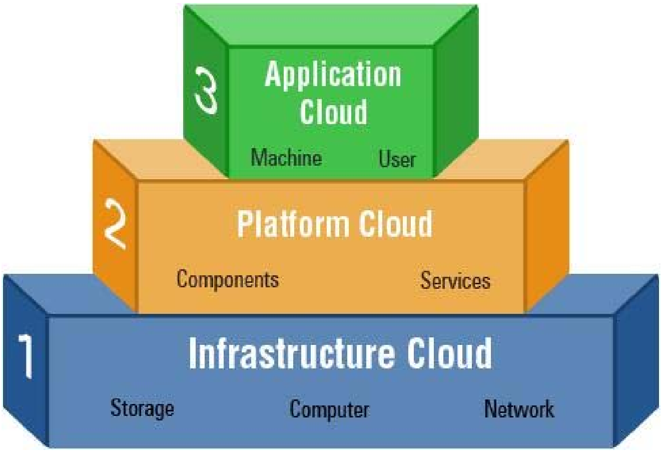


Figure 2.Cloud Service Models [4]

2.3 BENEFITS OF CLOUD COMPUTING

There are numerous benefits in cloud computing. Major ten benefits are explained below.

1, Cost Savings: Cloud computing provide facility to use services such as infrastructure, platform etc based upon requirements, it helps to reduce the initial cost, avoid the setting of high capacity servers and others that are capable of more than needy one. It charges amount depending upon usage of infrastructure, platform and other services, this helps consumers to reduce the expense by specifying the exact requirements.

2, Time Saving: Cloud computing reduce the set up time of organizations by providing all facility simultaneously. No need of waiting to set up the infrastructure, platform and others and avoid the initial headache. This helps organizations to save time, helps to run trial basis initially and gradually move to a permanent condition.

3, Scalability and Flexibility: As discussed in second benefit, companies can start with a small set up and grow to a large condition fairly rapidly, and then scale back if necessary. Also, the flexibility of cloud computing allows companies to use extra resources at peak times, enabling them to satisfy consumer demands. Moreover cloud computing is ready to meet any peak time requirement by setting up with high capacity servers, storages etc.

4, Backup and Recovery: Since all the 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 [10]. Also it has many techniques to recover it from any type of disaster.

5, Resource Maximization: Cloud computing has reduce burden of IT resources to many companies and agencies by maximizing the resources from cloud computing pool [12]. Most providers providing facility to meet any type of requirements at any time. This is one of the exciting feature of cloud computing.

6, Mobile Access: The cloud computing enables to access high- powered computing and storage resources for anyone with a network access device [13]. Employees can access and work on their application by sitting home, no need of going to office or organization. Moreover nowadays number of mobile users is very high compare to the users of PCs and other devices. Consumers can access their files and other applications anytime from anywhere by using their mobiles. This has increased the rate of adopting cloud computing technology.

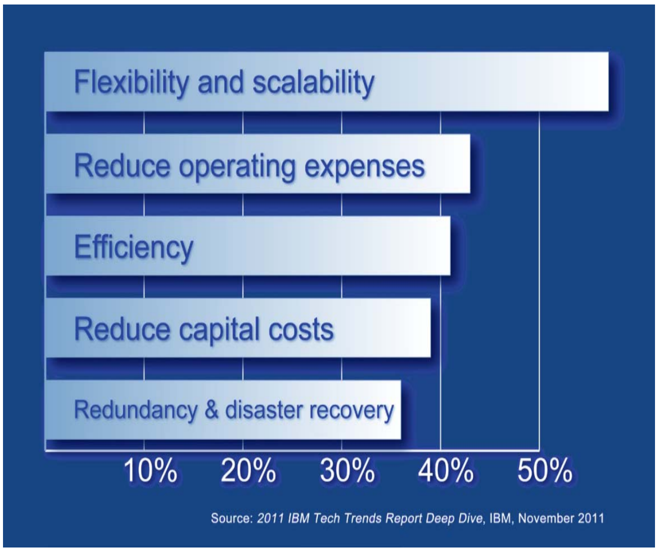
7, Multisharing: Cloud computing offers sharing of architecture and other applications for multiple users. With the cloud working in a distributed and shared mode, multiple users and applications can work more efficiently with cost reductions by sharing common infrastructure [14].

8, Customization: Cloud computing is a platform where we can modify to our needs with being redevelopment. It offers a platform for creating and amending applications to address a diversity of tasks and challenges [17].

9, Collaboration: Major projects or applications are delivering by the effort of multiple groups of employees working together. Cloud computing provide a convenient way to work group of people together on a common project or applications in an effective manner.

10, Deliver new services: Cloud services are provided by multi-national companies like Amazon, Google, IBM, Microsoft, Salesforce.com, etc. These companies can easily deliver any new application/product at the release time itself.

IBM's 2011 Tech Trends study shows where the improvements that Cloud offers are occurring first: In flexibility, scalability, and efficiency as well as reducing costs and providing the ability to ensure business continuity in the face of unanticipated disruption[15][16].



Source: *2011 IBM Tech Trends Report Deep Dive*, IBM, November 2011

2.4, SECURITY CHALLENGES OF CLOUD COMPUTING

There are many benefits as mentioned above, even though cloud computing has many challenges. While moving from owning site to cloud space, companies must aware about the benefits and challenges of cloud computing. While analysing these challenges, security of data is the most tedious work in cloud computing. According to a survey carried out by Gartner [7], more than 70% of Chief Technical Officers believed that the primary reason for not using cloud computing services is that of the data security and privacy concerns. Convincing the organizations especially small ones about security concern is a tedious work; they are not ready to throw away their infrastructure and immediate move to cloud. Most of the organizations are closely watching this issue and not ready to shift to cloud space, this is main reason in the lack of maturity level of cloud computing. Some of the security challenges are discussed below.

1, Privacy of data: Privacy of data is key concern for cloud computing. Most of organizations feeling more comfort while putting valuable data in their site than cloud. Consumers do not have any idea regarding the location of data, transfer of date, operations on cloud, etc. Many questions are arising by consumers such as

1. Which are the other organizations sharing services.
2. How creation and deletion of files taking place.
3. What about the back-up of data.
4. Which type of consumers can access data.
5. Location of data.
6. Etc.

2, Confidentiality of data: Confidentiality is related to data privacy, ensuring that the data is visible to only authorised users. It is very difficult due to the virtualization and multi tenancy properties that multiple consumers sharing the hardware, software simultaneously in a distributed network. Providing confidentiality is the responsibility of service provider. Common solution to the confidentiality is encryption. Many symmetric and asymmetric algorithms are available for data confidentiality, even though encryption and decryption is the solution to the confidentiality, there are many questions are arising related to this.

1. Where is encryption and decryption taking place (client side or cloud side).
2. How can search data in an encrypted form.
3. What are threats while transferring data from client to cloud?
4. Any miss use of data by service provider.
5. Any miss use of keys by service provider.
6. Etc.

3, Data Remanence: Data stored in the cloud must be deleted after its life-cycle, or the memory should be reformatted or recycled. The reformatting of storage media does not remove the previously written data from the media, but it can be accessed or recovered from the media later. No clear standard is available for recycle the storage media. This data remanenece makes difficult the vacation of hardware resources from the cloud. Most consumers are unknown to allotted resources and storage space, due to this issue consumers are locked in one service provider. Various techniques have been developed to counter data remanence. These techniques are classified as cleaning, purging/sanitizing, or destruction. Specific methods include overwriting, degaussing, encryption, and media destruction [19].

4, Data integrity: Preservation of information from loss or modification by unauthorized users is referred as data integrity. Multiple organizations are sharing the application or platform by multi-tenancy, consumers working on same work may share data can be modified by any other unauthorised user sharing the application or platform in the cloud, this cause the integrity failure. As data are the base for providing cloud computing services, such as Data as a Service, Software as a Service, Platform as a Service, keeping data integrity is a fundamental task [20].

5, Transmission of data: Most of time data is transferring between consumer and cloud. Initially data is sent from client site to cloud, data is returned from cloud to client after queries. Encryption is used provide protection while the transmission of data. Most of the time data is transferred without encryption due to lot of time is required for encryption and decryption for each operation upon data. During transfer an attacker can trace the communication, interrupt the data transfer, miss use of data, etc. Homomorphic algorithm allows processing data in an encrypted form, even though there is a chance of data transfer interruption, change the data transfer, other issues.

6, Data Breaches: As mentioned above, cloud environment is shared by multiple users and organizations of various part of the world; their valuable data is stored in one place. Any break or problem on cloud may expose these sensitive data to the users of other organizations sharing same storage. Because of multi-tenancy, customers using different applications on virtual machines could share same database and any corruption event that happens to it is going to affect others sharing the same database [21]. In [22], it was reported”2011 Data Breach Investigations Report” that hacking and malware are the common causes of data breaches, with 50% hacking and 49% malware.

7, Availability: Availability of cloud computing system for all time from anywhere is very important for the success cloud computing. Most of the IT solutions require services on all time due to critical services they provide, any interruption in service may cause loss, loss of consumer confidence. Attacks like denial-of-service are typically used to deny availability of data. If an attacker uses all available resources, others cannot use those resources, which leads to denial of service and could slow accessing those resources [9]. Also, customers, who are using cloud service and affected by botnet, could work to affect availability of other providers. Two strategies, say hardening and redundancy, are mainly used to enhance the availability of the cloud system or applications hosted on cloud [5].

8, Malicious Insiders: Malicious insiders are authorised employees, these users appointed for managing and maintaining cloud by cloud service provider. These users sometimes steal or corrupt the sensitive data of organizations in the cloud and convey this sensitive information to other organizations sharing the same cloud. These malicious insiders may get payment for this malicious work. Sometimes service provider not able to take any action against these employees.

9, API issues: Application Program Interface (API) is used for the communication between the cloud service and consumer site. API is used to manage and control data in the cloud. There is any failure on this API may lead to the security issues. If they are weak and security mechanism cannot defend them, this could lead to accessing resources even as privileged user [9]. Failures issues around API calls are a large source of faults that could lead to application failures, especially during sporadic activities. Infrastructure outages can also be greatly exacerbated by API-related issues. There are many solutions proposed [23] to avoid insecure interfaces and APIs:

1. Analysing the security model for interfaces of the cloud provider
2. Making a strong access control and authentication when data is transmitted
3. Understanding dependencies in API

10, Data location: Cloud Computing offers high degree of data mobility. Most Consumers do not know the location of their data. In most cases, this does not matter. For example, emails and photo graphs uploaded to Facebook can reside anywhere in the world and Facebook members are generally not concerned but while storing sensitive data, organization want to know the storage location [24]. Some organizations may prefer to store data in their country or jurisdiction. There are regulations in some countries where the company can store their data. Also, the data location matters when the user data is stored in a location that is prone to wars and disasters [9]. For example, Indian organizations don't want to store data in china jurisdiction similarly Chinese organizations don't want to store data in India jurisdiction.

11, Data Relocation: Movement of data from one location to another is a major issue. Initially data is stored in a particular location with the consent of organization but some situation provider may change the data location from one place to another due to unavoidable situations. But data location may be specified in the contract itself; it makes trouble to the movement of data.

12, Account or Service Hijacking: Users are using passwords to access the cloud service resources so when their accounts are hijacked and stolen, the passwords are misused and altered unsurprisingly [21]. The unauthorized user who has a password can access the clients’ data by stealing it, altering it, or deleting it, or for the benefit of selling it to others. There are many solutions proposed [23] to avoid account or service hijacking:

1. Preventing users from sharing their credentials
2. Using a two-factor authentication system
3. Monitoring all activities to detect unauthorized access

13, Interoperability: Organizations may relay services of multiple cloud service providers at a time. In this case the platform of one application should be corporate with the platform of other, it is possible via web services but such web services are very complex. Moreover integration of services offered by different service providers are very difficult for the consumers, they are not able to feel the actual gain of cloud computing. For example, Amazon’s “Simple Storage Service” [S3] is incompatible with IBM’s Blue Cloud, or Google, or Dell [25][26][27][28].

III. CONCLUSION

Cloud computing is world emerging, next generation technology in information technology. This technology offers variety of benefits to the relying organizations. In this paper I have discussed various benefits and service models of cloud computing in detail. Moreover I have highlighted the major security issues of this technology in most aspects. Here I conclude that, even though it has lot of benefits, it is suggesting you to adopt cloud computing services only after analysing all the major security issues in cloud computing.

REFERENCES

[1] Foster, I. T., Zhao, Y., Raicu, I., & Lu, S. (2009). *C*loud Computing and Grid Computing 360-Degree Compared CoRR. abs/0901.0131.

[2] Pranita P. Khairnar., Prof. V.S. Ubale, "Cloud Computing Security Issues And Challenges" I*nternational Refereed Journal of Engineering and Science*, vol. 03, 2009

[3] Satyakam Rahul, Sharda, "Cloud Computing: Advantages and Security Challenges" *International Journal of Information and Computation Technology,* vol. 03, 2013

[4] K.Kavitha , "Study on Cloud Computing Model and its Benefits, Challenges " , International Journal of Innovative Research in Computer and Communication Engineering, vol. 02,2014

[5] Santosh Kumar and R. H. Goudar, "Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey", International Journal of Future Computer and Communication, vol. 04, 2012

[6] Tharam Dillon, Chen Wu and Elizabeth Chang, "Cloud Computing: Issues and Challenges", *IEEE International Conference on Advanced Information Networking and Applications,* 2010

[7] Gartener: Seven cloud-computing security risks. InfoWorld.2008-07-02. http://www.infoworld.com/d/security-central/gartener-seven-cloud- computing-security-risks-853.

[8] http://www.keane.com/resources/pdf/WhitePapers/Cloud-Computing-Risks-and-Benefits.pdf

[9] Sultan Aldossary, William Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions", International Journal of Advanced Computer Science and Applications, Vol. 7, 2016

[10] Anca apostu, Florina puican, Geanina ularu, George suciu, Gyorgy todoran, "Study on advantages and disadvantages of Cloud Computing – the advantages of Telemetry Applications in the Cloud", *Recent Advances in Applied Computer Science and Digital Services*

[11]. Gaoyun Chen, Jun Lu and Jian Huang, Zexu Wu,"SaaAS - The Mobile Agent based Service for Cloud Computing in Internet Environme", Sixth International Conference on Natural Computation, ICNC 2010, pp. 2935-2939, IEEE, Yantai, Shandong,China, 2010. ISBN: 978-1-4244-5958-2.

[12] Cloud Computing Building a Framework for Successful transition, http://www.gtsi.com/cms/documents/White-Papers/Cloud-Computing.pdf

[13] Ajith Singh. N, Vasanthi.V, M. Hemalatha, "A Brief Survey on Architecture, Challenges & Security Benefit in Cloud Computing", *International Journal of Information and Communication Technology Research,* vol. 2, 2012.

[14] Srinivasa rao v, Nageswara rao n k, E Kusuma kumari, "Cloud Computing: An Overview", *Journal of Theoretical and Applied Information Technology.*

[15] 2011 IBM Tech Trends Report Deep Dive, IBM, November 2011, https://www.ibm.com/developerworks/mydeveloperworks/groups/service/html/communityview?communityUuid=ff67b471-79df-4bef-9593-4802def4013d#fullpageWidgetId=W90e0c883 70ed_487f_9118_c24512493b8f&file=a91dcf57-15c0-48c5-b0fa-21872b1365ff

[16] Quest Technology Management for Business, "The Benefits and Challenges of Cloud Computing",*www.questsys.com*.

[17] Cloud Computing Building a Framework for Successful transitin, http://www.gtsi.com/cms/documents/White-Papers/Cloud-Computing.pdf.

[18] Cloud computing security, http://in.wikipedia.org/wiki/cloud_computing_security.

[19] Data Remanence, https://en.wikipedia.org/wiki/Data_remanence.

[20] Vijay Kumar, "Brief Review on Cloud Computing", International Journal of Computer Science and Mobile Computing, vol. 5, September 2016,

[21] *CSA, "*The notorious nine cloud computing top threats in 2013*," TheN otoriousN ineC loudC omputingT opT hreatsi n2 013.pdf.*

[22] *W.Baker, "M," 2011 data breach in-vestigations report,"." [Online]. A vailable: http://www.wired.com/imagesb logs/threatlevel/2011/04/V erizon−[45]2011−DBIR04−13 − 11.pdf*

[23] D. Hubbard and M. Sutton, "Top threats to cloud computing v1. 0," *Cloud Security Alliance*, 2010.

[24] Puneet Kumar, Harwant Singh Arri, "Data Location in Cloud Computing",*International Journal for Science and Emerging Technologies with Latest Trends,5* (1): 2013

[25] L. Ertaul, S. Singhal, G. Saldamli, "Security Challenges in Cloud Computing",

[26] George Reese, "Cloud Application Architectures", First edition, O'Reilly Media, April 2009, ISBN 9780596156367, pp. 2-4, 99-118.

[27] John W. Rittinghouse, James F. Ransome, "Cloud Computing Implementation, Management, and Security", CRC Press, August 17, 2009, ISBN 9781439806807, pp. 147-158, 183-212.

[28] Amazon White Paper, "Introduction to Amazon Virtual Private Cloud", Available: http://aws.amazon.com/about-aws/whats-new/2009/08/26/introducing-amazon-virtual-private-cloud/.