International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT206489

A Comprehensive Review on Cloud Computing and Cloud Security Issues

Supongmen Walling
Department of Computer Science and Engineering, Indian Institute of Engineering Science and Technology, Howrah, West Bengal, India

Article Info
Volume 6, Issue 4
Page Number : 483-490
Publication Issue :
July-August-2020

Article History
Accepted : 15 Aug 2020
Published : 22 Aug 2020

ABSTRACT

Cloud computing is a type of computing where computing services such as applications, storage, infrastructure, processing power are hosted by some vendors (cloud vendors) over the Internet and delivered to users on on-demand basis. A company can benefit from cloud computing in the sense that they can rent access to anything from applications to storage to processing power rather than owning their own IT infrastructure. By using cloud-computing services, companies can avoid the various costs and complexities associated with owning and maintaining their own IT infrastructure as everything is taken care of by the service providers. Cloud computing is a paradigm in which both the users and the service providers are benefited. Service providers are greatly benefited from cloud computing by providing cloud services to a wide range of customers. The primary objective of this paper is to give an overview on cloud computing encompassing its features, the pros and cons of cloud computing and the challenges that comes with it. Furthermore, this paper also presents a list of security concerns in cloud computing which stands in the way of wide spread adoption of cloud computing thereby motivating researchers to devise competent solutions to tackle these ongoing security issues.

Keywords: IaaS, Cloud service provider, PaaS, SaaS, DoS.

I. INTRODUCTION

Cloud computing is gaining a lot of popularity among different businesses and has the potential to change the way businesses operate. It is the new buzz and has taken the market by storm. Cloud computing delivers application and IT capabilities as a service over the Internet using third party. Resources (CPU, storage etc.) are delivered as general utilities that are leased and released by user over Internet in pay-as-you-go and on demand basis. It is very attractive for business owners who can start from small and increase resources only if there is rise in service demand. Many different businesses and organization have adopted the concept of the cloud computing. Cloud computing enables consumer and businesses to use application without installation and they can access their files on any computer through Internet [1]. Currently, many Information Technology (IT) companies like Google, Yahoo, Amazon, etc. are providing cloud services to the users [2].

There are few requirements for cloud services:

- For accessing any data or services, the cloud service provider (CSP) must specify the access control policies.
- To provide a requested resource to the user, there must be a mapping of access policies

between the CSP and organizations with the available resources. There is always a chance to violate the mapping of policies. So, enforcing of more access policies by the organization are beneficial in regard to secure accessing of resources.

- The Data Owner (DO) must offer all kind of data services to the consumers [2].

1) Features of Cloud Computing

On-demand Service: Computing resources such as storage, processing power, applications etc are provisioned to users as and when needed and they only pay for what they use.

Work from Anywhere: As long as users have access to the Internet, cloud users can access the cloud and work on it from any location.

Cost Savings: By using cloud services, a company can avoid upfront cost and the complexities of owning and maintaining its own IT infrastructure because they are no longer required to purchase their own hardware but instead use web based services.

Updates: updates on software and other technical issues are no longer a headache to the consumers as everything is taken care of by the service providers.

Scalability: Cloud services are highly scalable and consumers can scale their resources up and down as and when they need according to their requirements.

2) Advantages of Cloud Computing

The benefits of using cloud computing are:

- **Cost Benefits:** Since cloud computing removes the need to own and maintain physical hardware and IT infrastructure, a user can save significant capital cost. Also cloud computing is pay as you go service so the user pays for only what he has used.
- **Updates and Maintenance:** all the updates and maintenance are done by the service provider so the user need not waste time on maintaining the system.
- **Easy Accessibility:** Cloud services are easily accessible from anywhere as long as you have a steady Internet connection.
- **Highly Available:** cloud services are highly available and reliable with most of them available with an uptime of 24x7.
- **Highly Scalable:** cloud services are highly scalable and so consumers can add resources or discard them according to their requirements.
- **High Reliability:** could runs on multiple servers so even in the case that one server fails, it is easily backed up and resources are pooled from other servers ensuring smooth and uninterrupted operation.

3) Disadvantages of Cloud Computing

- **Security:** Data security and privacy is one of the main disadvantages of cloud computing. By using cloud services, a user is storing all his data on the cloud which is basically someone else's computer. Some data are too sensitive to be placed on the cloud so there is always a concern for data privacy.
- **Downtime:** this means the time when the cloud is inactive due to service providers facing difficulties such as power loss, technical issues, and server maintenance.
- **Connectivity Reliance:** cloud computing is reliant on Internet connection and requires businesses or users to have stable Internet connectivity to use its services. Also when the service provider experiences loss in connectivity, no transactions can take place.
- **Limited Control:** When a company or an individual moves their data to the cloud, they have limited control over it due to the fact that all the back end activities are managed by the service provider and the user only has control over the front end of applications.

II. CLOUD DEPLOYMENT MODELS

There are generally four types of cloud; they are private cloud, public cloud, hybrid cloud and community cloud. Deployment depends on who controls the infrastructure and where it resides.

Private Cloud: A private cloud is a cloud infrastructure which is owned and operated by a single organization. It is not available to the general public and only the organization owning it and its members can access its resources. It is also called internal/ corporate cloud for this matter. A private cloud is more secure, reliable and maintains privacy as only authorized persons can access it.

Pros:

- Highly secure and reliable.
- It offers high level of customization.

Cons:

- In order to use private cloud, a company has to spend considerable expenses on hardware, software and staff training.

Public Cloud: Public cloud as the name suggests is available to the general public. In the public cloud, the cloud service provider provides the resources, such as network, server, etc. The server infrastructure belongs to the provider and so users/ companies need not buy and maintain their own individual hardware. Here, users can pay money for how much they have used the public cloud. In the public cloud, customers or users from many organizations are mixed together, and they use the same cloud or network [3].

Pros

- It is highly scalable.
- It is cost effective as the users pay for only what they use.
- Hassle free infrastructure management as all updates and maintenance are done at the server side by the service provider.

Cons:

- Data security is a concern.
- Less reliable.

Community Cloud: Community cloud is a collaborative effort in which the infrastructure and resources are shared by several organizations with similar background and interests. These clouds are generally based on an agreement between related business organizations and are managed by all these organizations jointly or by a third party.

Pros:

- It is cost efficient.
- It offers easy data sharing and collaboration.

Cons:

- Cost is higher compared to public model.
- Sharing responsibilities among organizations is difficult.

Hybrid Cloud: Hybrid cloud is a combination of the above mentioned deployment models (public, private, community) which exploits the best features of each model. For instance, a company using hybrid cloud can store its critical data in private cloud and store less sensitive ones in a public cloud. Hybrid Cloud provides more secure control of the data and applications and allows various parties to access information over the Internet.

Pros:

- It offers improved security and privacy.
- It has enhanced scalability and offers flexibility.

Cons:

- Initial setup cost is high.
- Compatibility issues

	Public	Private	Community	Hybrid
Ease of setup and use	Easy	Requires IT proficiency	Requires IT proficiency	Requires IT proficiency
Data security and privacy	Low	High	Comparatively high	High
Data control	Little to none	High	Comparatively high	Comparatively high
Reliability	Vulnerable	High	Comparatively high	High
Scalability and flexibility	High	High	Fixed capacity	High
Cost-effectiveness	The cheapest one	Cost-intensive, the most expensive one	Cost is shared among community members	Cheaper than a private model but more costly than a public one
Demand for in-house hardware	No	Depends	Depends	Depends

Figure 1. Comparative analysis on Cloud Deployment Models

III.CLOUD SERVICE MODELS

Cloud models are of three types namely SaaS (Software as a Service), IaaS (Infrastructure as a Service) and PaaS (Platform as a Service). Each of these models has their own benefits which can be used to satisfy different business requirements.

Software as a Service (SaaS): The most known and leading service model of more widespread adoption of cloud computing has been the SaaS [5]. This is an on-demand model where the user requests the service provider for various applications and software programs. It gives the user quick access to cloud based web applications. SaaS is a software delivery model that allows cloud service providers to host and maintain various web applications over the Internet to be accessed and used by end users. An example of SaaS is, these days you can choose to use Microsoft office by renting it from the service provider on a pay-per-use basis instead of purchasing its license and installing it on your system which is better in terms of flexibility and affordable enough for any budget.

Pros

- It is scalable.
- Easy Accessibility.
- Cost effective.

Cons:

- Requires stable Internet connection as SaaS is web based service.
- Security and privacy concerns.

Platform as a Service (PaaS): In this model, the cloud service provider delivers development environment/ platform to the user. The difference between SaaS and PaaS is that SaaS only hosts completed cloud applications where as PaaS offers a development platform for both completed and in-progress cloud applications [6]. PaaS is a develop and deploy environment in the cloud where users are given the resources to develop and deploy various apps ranging from simple cloud based to sophisticated ones. These application development resources are purchased from the services providers on pay-per use basis. The platform similar to SaaS is delivered over the web and all maintenance, updates, servers are managed by the service providers.

Pros:

- It is scalable and cost effective.
- Availability is high.

Cons:

- Data security is an issue.
- Dependency on Vendor.

Infrastructure as a Service (IaaS): IaaS offerings are computing resources such as processing or storage which can be obtained as a service [7]. It is a cloud computing service where end users lease storage, computing and storage resources from service providers. It allows companies to rent infrastructure rather than owning and managing its own infrastructure. IaaS model changes the way

developers deploy their applications. Instead of spending time with their own data centers or managed hosting companies, they can just select one of the IaaS provider, get a virtual server running in few minutes and pay only for the resources they use [8].

Pros:

- It is cost effective.
- It is the most flexible model.

Cons:

- Data security is an issue.
- If there is a failure/ interruption at vendor side, it would disrupt consumer activity.

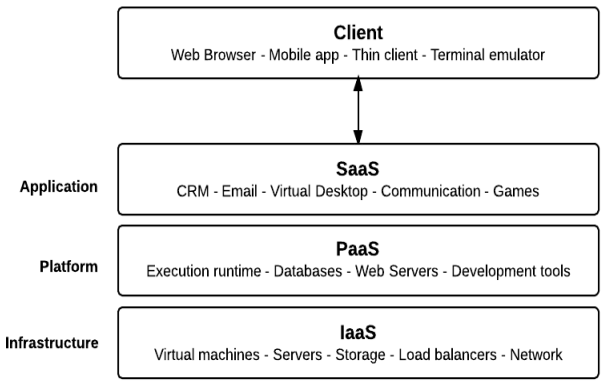

Figure 2. Types of Cloud Computing Service Models

IV. CLOUD COMPUTING CHALLENGES

Cloud computing is a very popular and an emerging technology today and is adopted by many companies and individuals but as popular as it may be, it has its fair share of challenges. In this section we address the various challenges faced by cloud computing.

Data privacy and Security: Data privacy is about securing the personal identifiable information (PII) of users. Personally identifiable information (PII) is any information that could be used to identify a particular individual. PII can be sensitive or non-sensitive. Non-sensitive PII is information that can be transmitted in an unhidden form. PII are easily found in the cloud computing services because of privacy issues [9]. Once a Cloud provider knows the PII (Name, Student number, Staff ID, Address, email and so on), it becomes a problem to the user. One of the most challenging issues that decrease the rate of reliability and efficiency in cloud computing environments is ensuring the security and privacy of stored resources. Cloud computing security has become an important topic in industry and academic research and has become the leading cause of impeding its development [10]. So, unless the vendor ensures data security and confidentiality by putting stringent security measures in place, cloud computing is not expected to be adopted by many.

Interoperability: This is the ability of two or more systems work together in order to exchange information and use that exchanged information. Many public cloud networks are configured as closed systems and are not designed to interact with each other. The lack of integration between these networks makes it difficult for organizations to combine their IT systems in the cloud and realize productivity gains and cost savings. To overcome this challenge, industry standards must be developed to help cloud service providers design interoperable platforms and enable data portability [11].

Data Protection: cloud protection is the practice of securing a company's data in a cloud environment. Data Security is a crucial element that warrants scrutiny. Enterprises are reluctant to buy an assurance of business data security from vendors. They fear losing data to competition and the data confidentiality of consumers. In many instances, the actual storage location is not disclosed, adding onto the security concerns of enterprises. In the existing models, firewalls across data centers protect this sensitive information. In the cloud model, Service providers are responsible for maintaining data

security and enterprises would have to rely on them [12].

Portability: portability means transferring the applications running on one cloud platform to another. However, applications deployed on one cloud platform including data and resources are difficult to move between clouds due to difference in platforms leading to issue in portability.

Performance**:** When a business moves to the cloud it becomes dependent on the service providers. The next prominent challenges of moving to cloud computing expand on this partnership. Nevertheless, this partnership often provides businesses with innovative technologies they wouldn't otherwise be able to access. On the other hand, the performance of the organization's BI and other cloud-based systems is also tied to the performance of the cloud provider when it falters. When your provider is down, you are also down [13].

V. SECURITY ISSUES IN CLOUD COMPUTING

When it comes to the cloud, data is stored at the service provider's side which is accessed over the Internet. The user has limited control over his data and visibility becomes restricted. There is also a question of how securely these data are stored and managed. Security issues in cloud are shared by both the provider and the customer. The service provider has to insure that services provided are secure and customer ensures that service that they are using is secure.

In this section we will look through the various security challenges faced by cloud computing.

Data Breach: data breach is a key security concern found in cloud computing. It is an incident where sensitive and confidential data are released to an unauthorized environment. Data breaches may occur due to a variety of reasons; it could be intentional or unintentional. It could be unintentional through data leaks, information leakage or intentional through theft.

Hijacking of accounts: account hijacking is a situation where a cloud user's account has been compromised by an attacker. It is a form of identity theft where the attacker has successfully acquired the credentials of the cloud user and uses the stolen account to conduct malicious activity. Attackers obtain user accounts through phishing by sending fake e-mails, web pages to targeted users or through the use of malicious software.

Insider Attack: insider attack also known as turn cloak is an attack where someone from the organization maliciously tries to access confidential information. Insider attacks are the realization of the risk to companies, their data, their business partners and their long-term future caused by insiders becoming malicious and acting upon it. These attacks are orchestrated or executed by people that are trusted with varying levels of access to a company's systems and facilities, and who have intimate knowledge of the company's infrastructure which an external attacker would take a significant period of time to develop [14].

Denial of Service Attacks: Unlike the other forms of attacks which try to hijack sensitive information, denial of service is an attack meant to shut down website or servers rendering it useless for legitimate users. In cloud computing, a DoS attack can be described as an attack designed to prevent some cloud computing service or resource from providing its normal service for a period of time. DoS attacks compromise the availability of the cloud resources and services and often target the computer networks bandwidth of connectivity [15]. The attacker shuts down the servers, networks and machines of target

organizations rendering it inaccessible to its legitimate users by flooding it with unwanted traffic.

Data Loss: data loss is a situation where information systems storing information is destroyed leading to loss of vital information. Information system can be destroyed as a result of negligence, mishandling, natural disasters, and malicious attacks or due to a data wipe by the service provider intentionally or unintentionally. This could heavily affect businesses which do not have a recovery plan. Amazon suffered data loss in 2011 by destroying many of its customer's information. Google is another organization that suffered massive data loss when its power grid was struck by lightning.

VI. CONCLUSION

Cloud computing is one of the fastest growing areas in the IT field today offering tremendous benefits to customers of all types and sizes. It is one of the major enabler for so many companies and organizations. Cloud computing is so popular today as it offers a wide array of services at affordable rates and cloud solutions are so much simpler to acquire, they don't require long term contracts and can be scaled up and down as required. With all the benefits that it is offering, cloud computing do have its own share of disadvantages and challenges, and active researches are underway in order to address the various issues faced by cloud computing.

VII. REFERENCES

[1] Divya Kapil, Parshant Tyagi, Sonu Kumar, Vinay Prasad Tamta, "Cloud computing: overview and research issues", In the proceedings of 2017 International Conference on Green Informatics (ICGI 2017), China, Vol. 1, pp 71-76, 2017.

[2] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the art and research challenges", Journal of Internet Services and Applications, Vol. 1, pp. 7-18, 2010.

[3] Suyel Namasudra., Pinki Roy., Balamurugan Balusamy, "Cloud Computing: Fundamentals and Research Issues", In the Proceedings of 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM 2017), India, Vol.1, pp 7-12, 2017.

[4] Best Cloud Deployment Models You Need to Know. https://www.sam-solutions.com/blog/four-best-cloud-deployment-models-you-need-to-know/.

[5] Michael H. Hugos, Derek Hulitzky, "Business in the cloud: what every business needs to know about cloud computing", Wiley, 2010.

[6] Peter Mell, Tim Grance, "NIST definition of cloud computing, National Institute of Standards and Technology", 2011.

[7] Shyam Patidar, Dheeraj Rane, Pritesh Jain, "A Survey Paper on Cloud Computing". In the Proceedings of 2012 Second International Conference on Advanced Computing & Communication Technologies (ACCT 2012), USA, pp 394-398, 2012.

[8] Subashini S, Kavitha V, " A survey on security issues in service delivery models". Journal of Network and Computer Applications Vol. 34, Issue 1, pp 1-11, 2011.

[9] Pearson S. "Taking account of privacy when designing cloud computing services", In the Proceedings 2009 of ICSE Workshop on Software Engineering Challenges of Cloud computing, Vancouver, pp 44-52, 2009.

[10] S. Chaves, C. Westphall, C. Westphall, and G. Geronimo. "Customer Security Concerns in Cloud Computing". In the Proceedings of 2011 10th International Conference on Networks (ICN 2011), The Netherlands, pp 7-11, 2011.

[11] Mohsin Nazir, "Cloud computing: overview and current research challenges". IOSR Journal

of Computer Engineering (IOSR-JCE) Vol. 8, Issue 1, pp 14-22, 2012.

[12] Gurmeet Singh, Vineet Kumar Sachdeva, "Impact and challenges of cloud computing in current scenario". International Journal of Social Science & Interdisciplinary Research, Vol.1, Issue 10, 2012.

[13] Cloud Computing Risks and Challenges. https://www.datapine.com/blog/cloud-computing-risks-and-challenges/.

[14] Adrian Duncan, Sadie Creese, Michael Goldsmith, "Insider Attacks in Cloud Computing", In the Proceedings of 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, England, 2012.

[15] Mohammad Masdari, Marzie Jalali, "A Survey on taxonomy of DoS attacks in cloud computing", Security and Communication Networks, Wiley Online Library, Vol 9, pp 3724-3751, 2016.

Cite this article as :

Supongmen Walling, "A Comprehensive Review on Cloud Computing and Cloud Security Issues ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 4, pp. 483-490, July-August 2020. Available at doi : https://doi.org/10.32628/CSEIT206489
Journal URL : http://ijsrcseit.com/CSEIT206489