UGC APPROVED JOURNAL - 47746
INNOVATIVE RESEARCH THOUGHTS | Refereed | Peer Reviewed | Indexed
ISSN : 2454 – 308X | Volume : 04 , Issue : 03 | January – March 2018

A study of Advantages and Disadvantages of Cloud Computing

Shalini

Email id- shaliniruhil@gmail.com

Abstract

The cloud or virtual space in the name of this type of computing refers to the location from which data is accessible. Companies offering cloud services make it possible for customers to backup "their data and programmes to remote servers and then access it through the Internet. So, the user may access it from wherever they happen to be, eliminating the need to physically be in close proximity to the system. When you use cloud computing, your mobile or desktop device doesn't have to do any of the grunt work of data processing. This process also offloads the laborious task to hordes of remote computers. With the Internet serving as the cloud, all of your information and programmes can be accessed from any Internet-connected device, no matter where you are.

Key words: Cloud, Computing, Modern, Technology, IaaS, SaaS etc.

Introduction

Computing resources (such as networks, servers, storage, applications, and services) can be rapidly deployed and delivered on demand through the use of cloud computing with minimal intervention from the service provider or IT staff. Conventional approaches to data centre and business application development and maintenance are being tested by the rise of cloud computing. In light of this new deployment paradigm, the efficacy and efficiency of traditional preventative measures are being reexamined. Using the same security concepts as multi-user mainframe security, cloud security may be thought of as an example of applied security. Whether a service is hosted in the public or private cloud, it will always require some sort of oversight. Cloud service providers have a lot riding on the success of their efforts to improve cloud security. Data isolation, privacy, exploiting and recovering from bugs, insider dangers, management console security, and account administration are all issues that need to be addressed. Cryptography, PKI, numerous cloud providers, consistent APIs, and increased virtual machine support are all viable solutions to the security problems associated with the cloud. The TDT4 and privilege methods were developed with input from the crypto and IR communities to meet the system's security and usability requirements.

Types of Cloud Computing

As opposed to a microprocessor or a mobile phone, cloud computing is a collection of interconnected technologies. Software as a service (SaaS), infrastructure as a service (IaaS), and a platform as a service (PaaS) make up the bulk of this system (PaaS).

- Customers are granted a licence to use a certain piece of software through a service known as software as a service (SaaS). Typically, licences are made available on a subscription or pay-as-you-go basis. Microsoft Office 365 is one example of such a system.
- The term infrastructure as a service (IaaS) refers to the practise of offering a variety of computing resources—from operating systems to servers and storage—over an IP-based network as an instantaneous service. Customers can avoid spending money on software and hardware by renting or leasing it through an on-demand service. IBM Cloud and Microsoft Azure are two well-known implementations of the IaaS model.
- When comparing the three levels of cloud computing, platform-as-a-service (PaaS) is often regarded as the most sophisticated. While comparable to SaaS in some ways, PaaS differs in that it is a platform on which to build and distribute software over the Internet, rather than simply providing software over the Internet. Sites like Salesforce.com and Heroku are examples of platforms that fit this mould.

Advantages of Cloud Computing

The ability to access and utilise software from anywhere, using either a native app or a browser, is just one of the many advantages cloud computing brings to businesses of all sizes and in all industries. Thus, consumers are able to seamlessly transfer their data and preferences between devices.

A simple example of cloud computing is the ability to access data from various devices. Users may access their email from any computer and save files to cloud services like Dropbox or Google Drive.

Additionally, cloud services enable users to create backups of their data, such as movies and documents, making them quickly accessible in the case of a hardware failure.

There is a substantial opportunity for cost savings, especially for large organisations. Companies previously had to spend a lot of money on expensive hardware and software

for managing data on-premises before cloud computing became an option. In place of expensive data centres and IT staffs, businesses may instead rely on reliable Internet connections and have their workers perform their work in the cloud.

Because of the cloud's design, users may free up disc space on their computers. By distributing their wares through the internet as opposed to the more time-consuming and cumbersome process of shipping CDs or flash drives, software businesses make it possible for consumers to update to newer versions of their programmes more rapidly. Adobe, for instance, offers its Creative Cloud subscription service where users may gain access to the company's suite of web-based apps.

This facilitates the distribution of updates and bug fixes for software to end users.

Disadvantages of the Cloud

There are benefits to using cloud computing, such as increased speed and efficiency, as well as new and exciting developments. However, there are also hazards involved.

When it comes to personal information such as bank accounts and medical records, cloud security has always been a major worry. Cloud services continue to struggle with this issue, even as rules require providers to increase their security and compliance procedures. Although encryption is effective at protecting sensitive data, it is useless if the key to decrypting the data is lost.

Disasters, faulty software, and power outages are just some of the threats that might affect cloud providers' servers. A power outage in California might render New Yorkers helpless, and a company in Texas could lose data if something caused its provider in Maine to fail.

There is a learning curve associated with this technology for both employees and supervisors. However, when several users access and update data through a single interface, faults made by one user might propagate throughout the whole system.

Private Cloud

Within the confines of the company's firewall is a private cloud managed by the IT staff. More control over sensitive company and customer data, as well as less concerns about security and compliance issues, are just two of the many advantages of using a private cloud versus a public one.

Public Cloud

The term public cloud refers to a model in which a third-party service provider makes its infrastructure, including hardware, software, and data storage, available to anybody with an Internet connection. It is possible to use public cloud services on a pay-as-you-go basis.

Hybrid Cloud

Those that can't be handled locally are sent to a hybrid cloud. While active client data is kept in-house, the company may use a public cloud service like Amazon S3 to retain historical data. Organizations may choose a hybrid model to take advantage of the scalability and low cost of public cloud computing. Hybrid information technology is another name for this idea. A solid method for managing a hybrid cloud environment will incorporate allocation of funds, administration of modifications, and protection against unauthorised access. It is possible to construct a hybrid cloud, which combines public cloud and private data centre concepts, from any of these locations. If the organisation is serious about reaching its objectives, it needs to pick the right place to begin. When it comes to internal business processes, a hybrid cloud brings together the best of both the private and public cloud worlds. All cloud computing services should be effective, although public clouds are expected to be less expensive and more scalable than private ones.

Hybrid cloud models can be implemented in a number of ways:

- Each cloud service provider contributes to a unified product.
- All the pieces for a hybrid cloud environment may be found with only one cloud service.
- Public cloud services are utilised by companies that have their own private cloud infrastructures.

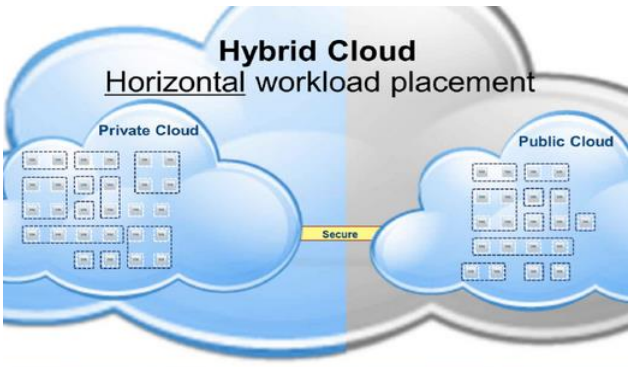

Fig: Hybrid cloud

Challenges of Cloud Computing

When it comes to the cloud, security is the only real issue. Consumers are worried about their data being compromised due to cloud computing's meteoric rise. While there are numerous upsides to cloud computing, there are also some potential dangers. The risk posed by individuals and organisations without proper authorization is growing. Because of this necessity, cloud computing has created a new technique for sharing information across many users, each of whom may retrieve just the files they require at any one time.

- Customers have no way of knowing what goes on within the cloud since it is pitch black.
- Users of cloud services typically have little insight into and management of cloud processes.
- If the cloud provider is trustworthy, a rogue system administrator might nevertheless compromise the security of the virtual machines (VMs) in their care.
- Concerns about data security, privacy, and availability in the cloud are not new but persist nonetheless.

Companies are still afraid to use clouds

Most security flaws result from: - Loss of control

There are two main concepts here: - Intrust (mechanisms) - Multi-tenancy.

These worries are mostly attributable to outsourcing management.

– Despite addressing the aforementioned vulnerabilities, self-managed" clouds remain at risk.

Literature Review

(Bonguet and Bellaiche 2017) studied "*A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing*" in which a shared set of highly adaptable resources is made available to all users at all times (e.g., networks, servers, storage, applications and services). The properties of the Cloud, such multi-tenancy and resource sharing, make it more susceptible to attacks like DDoS and DDoS, which threaten the availability of Cloud services.

(Lynch 2011) studied "*SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0*"in which all users have instantaneous, frictionless access through any available network to a central repository of programmable hardware and software (e.g., networks, servers, storage, applications, and services). Cloud computing

is a game-changing innovation that may enhance teamwork, agility, scalability, and availability while reducing overhead expenses.

(Sen 2013) studied "*Security and Security and Privacy Issues in Cloud Computing* " cloud computing promises better cost efficiency, increased innovation, shorter time to market, and the flexibility to grow applications on demand; it also alters the way IT is consumed and managed. Despite the fact that cloud computing was already a hot topic in 2008, its popularity skyrocketed that year and hasn't slowed down much since, it's obvious that there's been a fundamental paradigm shift toward this approach, and the advantages may be significant.

(Swapna et al. 2016) studied "*Performance Evaluation of Fuzzy Integrated Firewall Model for Hybrid Cloud based on Packet Utilization*" He found that Cloud computing is a fantastic method of sharing data globally. Network administrators are now confronted with data protection and vulnerability challenges while sharing data via cloud systems, prompting the development of cloud security measures. We may safeguard our data on a hybrid cloud by adjusting the settings of the network firewall.

(Mallika 2017) studied "*A Secured Decentralized Cloud Firewall to achieve Resources Provisioning Cost Optimization and QOS* " and discovered that the cloud is rapidly gaining traction as the IT sector's preferred choice for the next generation of computing infrastructure. Cloud computing delivers quick elasticity by pooling and delivering massive volumes of hardware and software resources on demand.

(Ullrich et al. 2016) studied "*The role and security of firewalls in cyber-physical cloud computing*" I learned that Clouds and other cyber-physical systems are here to stay. Due to these paradigm shifts, a new approach to security is required. Clouds do away with regional networks and instead route all internal traffic over the web. Cyber-physical systems are susceptible to cyber attacks since many of their physical components were meant to be used independently. Cloud computing in the cyber-physical realm introduces a new layer of safety.

(Yan et al. 2011) studied "*The Research and Design of Cloud Computing Security Framework*" , and it was discovered The popularity of cloud services has skyrocketed in recent years. Security concerns have slowed the adoption of cloud computing, but they are too important and pressing to ignore. In light of these issues, this research proposes a new security paradigm for cloud computing. It is recognised that the proliferation of

cloud computing and its variety of uses will continue only if the security concerns are resolved..

(Yeasmin et al. 2018) studied "*Performance evaluation of multi-cloud compared to the single-cloud under varying firewall conditions*" This article's major focus is to examine the differences between single-cloud and multi-cloud network performance behind different types of firewalls. The Riverbed Modeler simulation programme was used to create this set of projects.

Security of Digital Data in Cloud using Encryption mechanism

Information stored in the cloud has often been encrypted. On the other hand, cryptography is the study of secret forms of communication that can be understood only by the sender and the receiver. The term kryptos comes from the Greek word cryptos, from which the English word kryptos is derived. They have all the tools necessary to read and make sense of intercepted communications. The recommended study evaluates polynomial encryption against RSA and AES.

Conclusion

Numerous definitions and discussions about cloud computing have emerged in the information and communications technology industry recently. In cloud computing, a third-party company acts as a server, hosting data and applications for remote users. Innovations in computing, communication, and networking have pushed technology in this direction. A constant and rapid connection is necessary for cloud computing. Due to its low cost and tremendous flexibility, cloud computing is certainly one of the most alluring technical fields of today. Concerns about cloud computing are slowing its adoption and putting its viability as a new model for purchasing information technology at risk. Many potential customers have yet to sign up, and even those that do choose to use cloud computing for less sensitive data, despite the many financial and technological benefits that have been touted. When cloud implementation is irrelevant, loss of control means transparency, which runs counter to the original promise of cloud computing.

References

1. Bonguet, Adrien, and Martine Bellaiche. 2017. A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing. *Future Internet* 9(3). doi: 10.3390/fi9030043.
2. Lynch, Liam. 2011. Security Guidance for Critical Areas of Focus in Cloud. *Csa* 0–

176.

3. Mallika, T. M. 2017. A Secured Decentralized Cloud Firewall to Achieve Resources Provisioning Cost Optimization and QOS. 5(20):1–6.
4. Sen, Jaydip. 2013. Security and Privacy Issues in Cloud Computing. *Architectures and Protocols for Secure Information Technology Infrastructures* (iv):1–45. doi: 10.4018/978-1-4666-4514-1.ch001.
5. Swapna, Asma Islam, Ziaur Rahman, Md Habibur Rahman, and Md Akramuzzaman. 2016. "Performance Evaluation of Fuzzy Integrated Firewall Model for Hybrid Cloud Based on Packet Utilization." *2016 1st IEEE International Conference on Computer Communication and the Internet, ICCCI 2016* 253–56. doi: 10.1109/CCI.2016.7778919.
6. Ullrich, Johanna, Jordan Cropper, Peter Frühwirt, and Edgar Weippl. 2016. "The Role and Security of Firewalls in Cyber-Physical Cloud Computing." *Eurasip Journal on Information Security* 2016(1). doi: 10.1186/s13635-016-0042-3.
7. Yan, Xiaowei, Xiaosong Zhang, Ting Chen, Hongtian Zhao, and Xiaoshan Li. 2011. "The Research and Design of Cloud Computing Security Framework." *Lecture Notes in Electrical Engineering* 121 LNEE(January 2014):757–63. doi: 10.1007/978-3-642-25541-0_95.
8. Yeasmin, Mahbuba, Nahida Akter, Mohammed Humayun Kabir, and Javed Hossain. 2018. "Performance Evaluation of Multi-Cloud Compared to the Single-Cloud under Varying Firewall Conditions." *Cogent Engineering* 5(1):1–13. doi: 10.1080/23311916.2018.1471974.