Applied Science & Engineering Journal for Advanced Research
ISSN (Online): 2583-2468
Volume-1 Issue-2 || March 2022 || PP. 21-24 DOI: 10.54741/asejar.1.2.5

Security Challenges and Issues with Cloud Computing in IT Services

Bhanu Priya
Assistant Professor, Department of Computer Science, C.R.M Jat P.G College, Hisar, India

Corresponding Author: bhanupriya2001@rediffmail.com

Received: 03-03-2022 Revised: 09-03-2022 Accepted: 20-03-2022

ABSTRACT
Using cloud computing, we can get a variety of IT services, such as programme execution environments, application development environments, and data storage facilities, all from a single location over the internet, or "under one roof." On a leased basis, these services are provided to the customer. Apart from these features, there are numerous security concerns, as consolidating everything into the cloud makes it easier for hackers to gain access. Security is the most momentous roadblocks to the widespread adoption of cloud computing. An overview of cloud computing and its security challenges is provided in this paper.

Keywords: *cloud computing, cloud services, security issues, deployment models*

I. INTRODUCTION

The term "cloud computing" refers to the practise of renting or subscribing to a variety of IT services from a third-party provider over the internet. It gives customers the freedom to use services however they see fit. A few years ago, it became the new focus of business organisations because it provides online data storage, infrastructure and applications. It is a way to dynamically increase the capability and also add their aptitudes in a business without the need to invest in new infrastructure, training new employees, licencing new software, or maintaining the current infrastructure. Google docs and Google drive are examples of cloud-based services. [2] Centralizing storage, memory, processing, and bandwidth[3] allows for much more efficient computing[4]. The following characteristics (illustrated in diagram) characterise the cloud computing paradigm:

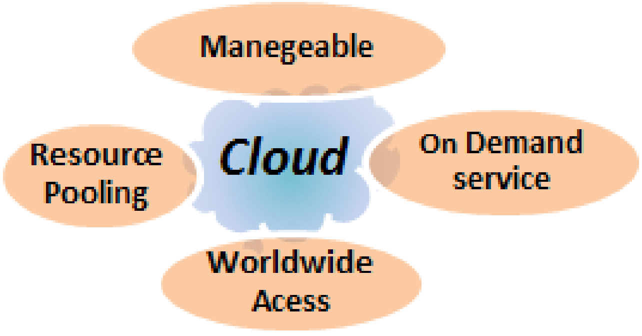

Figure 1: Features of cloud computing

1. **It's Managed:** On behalf of the customer, a third-party company provides and manages cloud computing services. Users don't have to be concerned about things like software upgrades or virus protection for their files.
2. **On- Demand Service**: For the services he needs, the user can request and pay only for those services.
3. **Worldwide Access**: As long as you have an internet connection, you can access cloud computing services from any location in the world.
4. **Resource Pooling**: With multiple rental or subscription strategies, cloud computing resources are pooled under one roof (i.e. cloud). Resources are dynamically scaled up and down in response to customer demand.

However, despite all of these advantages, the cloud computing service's most significant issue is the security. Customers or companies run the risk of compromising their own security by storing sensitive information on a third party's system in a foreign country. Cloud computing's growth is stifled by this. Sections of this paper are laid out in a logical order. Models for deploying the cloud are the focus of Section II. The cloud service models are discussed in Section III. In Section IV, we'll talk about security concerns. Section V of the paper outlines the paper's conclusion.

II. CLOUD DEPLOYMENT MODELS

The type of cloud deployment models customer chooses and implemented decides the level of security one gets:

2.1 Public cloud

In a public cloud, users pay a monthly fee to access the cloud infrastructure, which is then made available to everyone else. Public cloud services like Gmail and YouTube are the most well-known examples of this type of cloud computing. It's important to keep in mind that everyone using public cloud services has limited configuration options, making their data less secure.

2.2 Private Cloud

Private cloud computing is similar to public cloud computing, except that the resources can only be accessed via securez network connections. An secretive cloud organization is one that is exclusively used by an single organisation, giving that organisation greater security and control over their data. on-premises or by a third-party service provider (externally hosted or off-premise).

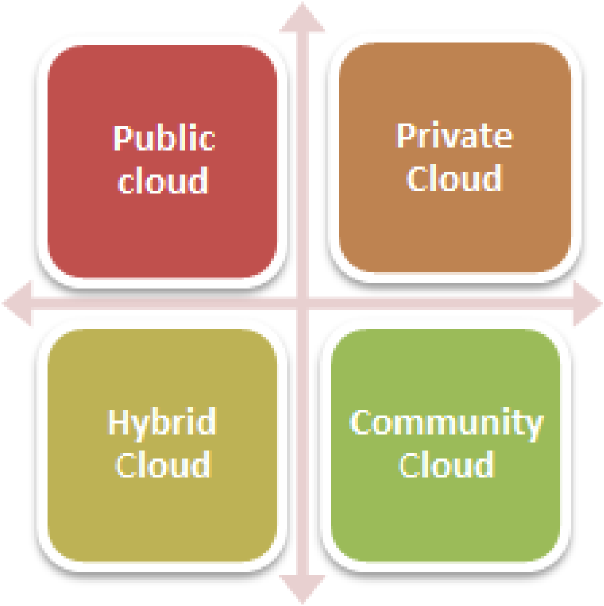

Figure 2: Types of Cloud deployment model

2.3 Crossbreed Cloud

Using a combination of private and public clouds, hybrid cloud computing allows businesses to take advantage of the best of both worlds by utilising the best of both worlds for some of their most critical functions while also utilising the public cloud for less critical ones.

2.4 Community Cloud

All of the participating organisations or a third-party managed service provider govern, manage and secure a community cloud infrastructure. Each of these organisations is based on the same technology and has a similar set of issues to address.

III. DELIVERY MODELS OF CLOUD COMPUTING

Three main cloud computing delivery prototypes are Infrastructure-as-a-Service (IaaS), the Platform-as-a-Service (PaaS) and the Software-as-a-Service (SaaS).

3.1 Infrastructure-as-a-Service (IaaS)

The Infrastructure-as-a-Service (IaaS) is the most basic form of cloud computing. Servers, storage, networking equipment (such as routers), and operating systems are all available as a service through Infrastructure as a Service (IaaS). Instead of purchasing these resources, you can simply call up a cloud service provider and have them delivered when you need them when you need them. This helps organisations save money.

3.2 Platform-as-a-Service (PaaS)

The Platform-as-a-Service occupies the middle ground. Platform-as-a-Service facilitates the rapid and efficient creation of software applications by providing a set of development tools and services. There are also applications-related services that can be hired.

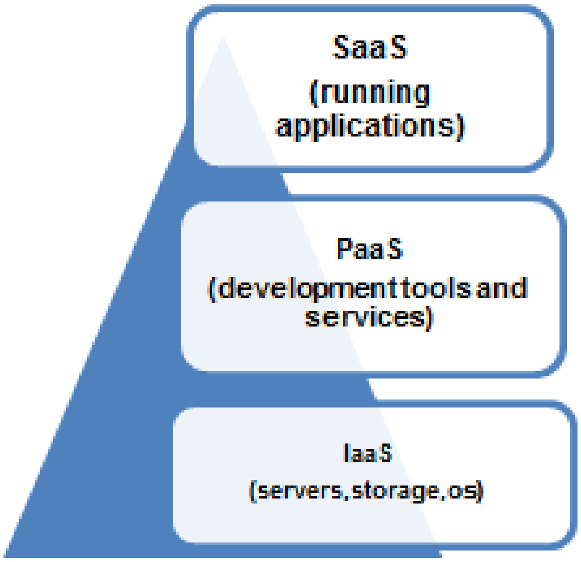

Figure 3: Delivery Models of Cloud Computing

3.3 Software-as-a-Service (SaaS)

The Software-as-a-Service (SaaS) occupies the highest position. Software and its functions can be accessed via web-based services such as email and Google docs in this model. Organizations can get into services at a fraction of the cost of purchasing licenced applications thanks to Software-as-a-Service. After the result of the software being hosted remotely, users are spared the costs and hassles of purchasing and setting up additional hardware.

IV. CLOUD COMPUTING SECURITY ISSUES

Cloud computing safety and privacy are major concerns. Many people find it intimidating to store their data on someone else's servers, run their programmes on someone else's CPUs, or create software using someone else's tools. Operating systems, networks and databases are among the many systems that make up cloud computing. It also includes features such as load balancing and currency control. Although there are numerous security concerns, we will only address a few of them in this article.

4.1 Information Confidentiality Issue

Data belonging to multiple customers may be stored on the same server in a cloud computing platform (hardware, operating system, and storage). When one customer's personal information is accidentally shared with another, there is a risk of information leakage.

4.2 Hyperjacking

Cybercriminals are devoting significant resources to finding ways to breach the cloud. It is theoretically possible for hackers to take over vast amounts of data by "hyperjacking" large cloud servers, which store data from a large number of different companies.

4.3 Data Availability Issue

When storing data in a third-party location, the data owner runs the risk of a service provider's system failing. Because it is dependant on a single service provider, the data will be unavailable if the cloud goes down. The objective of cloud computing is to deliver a variety of on-demand services. If a specific service is no longer available or if the excellence of service does not meet the Overhaul Level Agreement Customers may lose faith in the cloud system.

4.4 Lack of Verifying Client's Background

Anyone with a credit card and an email address can open a cloud account. A client's background is not typically checked by most cloud service providers. This gives the attackers the ability to carry out any malicious activity without being detected.

4.5 Data Theft

Customers' data is stored in the cloud on external servers, which may or may not be located outside the country. As a result, there is a possibility that data from the external server could be stolen.

4.6 Data Segregation

Security concerns arise when multiple companies store their data on the same server in encrypted form, so the provider should implement a mechanism to separate the data.

4.7 Data Loss

A user's data will be lost if the cloud computing service provider has to shut down because of a financial or legal issue. Misshapen, disasters natural and man-made, and fire all have the potential to corrupt or destroy data in transit. Users will be unable to access data because of the aforementioned issue.

4.8 Data Transparency Issue

Customers have no idea where their data is stored when they use a cloud service provider. Customers should be able to see what's going on.

There are two levels of security to consider when dealing with the cloud. One is for the service provider and the other is for the end user. In order to protect the server, the cloud computing service provider must be aware of all external threats. At the user level, the user should ensure that other cloud users do not suffer any data loss or theft or tampering as a result of its actions. Cloud computing security is a major issue, but there is no doubt that Cloud Computing has several benefits, including cost efficiency, automatic software upgrades, work from home, flexibility, unlimited storage, backup and recovery facility etc. Cloud Computing has a number of advantages.

V. CONCLUSION

Cloud services are becoming increasingly important in today's technologically advanced world because of their features and benefits. An overview of cloud computing and the deployment models and services it offers is presented in this paper before a discussion of the major security concerns that are impeding its expansion is offered. Cloud computing has the potential to lead the way toward a virtual, secure, and cost-effective IT solution in the near future. Network, data, storage, and other related security issues are the subject of ongoing research.

REFERENCES

1. Mell, Peter, & Tim Grance. (2009). The NIST definition of cloud computing. *National Institute of Standards and Technology*, *53*(6), 50.
2. Kuyoro S. O, Ibikunle F., & Awodele O. (2011). Cloud computing security issues and challenges. *IJCN*, *3*(5).
3. http://en.wikipedia.org/wiki/Cloud_computing.
4. D. Zissis, & D. Lekkas. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583-592.
5. N. Gruschka, L. L. Iancono, M. Jensen, & J. Schwenk. (2009). On technical security issues in cloud computing. In: *PROC 09 IEEE International Conference on Cloud Computing*, pp. 110-112.