IJARSCT

ISSN (Online) 2581-9429

IJARSCT
Impact Factor: 6.252

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 2, Issue 2, June 2022

Impact of Cloud Computing on the IT industry- Its Future and Security

Sana Mohammed Khalid Patel
Student, Department of Computer Application
Late Bhausaheb Hiray S S Trust's Hiray Institute of Computer Application, Mumbai, India

Abstract: *Cloud Computing, the long-awaited goal of computing as a service, has the capability to revolutionize a huge portion of the IT sector, making software even more appealing as a service. Cloud computing encompasses both the applications offered as services via the Internet as well as the hardware and software in the data centers that support such services. The offerings are referred to as "Software as a Service" (SaaS). Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) are two further forms of cloud computing services (PaaS). At the same time, cloud computing has decreased the cost of managing physical and technical infrastructures. After embracing cloud computing as a means for storing data, analyzing security frameworks, and ensuring privacy at the same time, the IT sector has witnessed significant growth. With the introduction of cloud computing. We will understand cloud computing and its influence on the IT industry in this document. We'll also learn about potential upcoming cloud computing developments in the IT sector.*

Keywords: Cloud Computing, IT Industry, SaaS, PaaS, IaaS.

I. INTRODUCTION

1.1 What is Cloud Computing?

The term cloud computing, the word cloud is an analogy for the internet. The word cloud is inspired by the old symbol of cloud which was often used to represent the Internet in flow charts. Through cloud computing, information systems resources that include applications, data, networks, storage devices, and servers are made accessible and available for use. A traditional setup will require you to be at the same place as your storage device. Cloud computing makes it easier to access data anywhere and at any time. You no longer need to be physically present where the hardware that keeps your data is by using the cloud. The term "cloud computing" refers to a method for providing easy-to-use network access to a shared on-pool of reconfigurable computing resources (such as networks, servers, storage, applications, and services) that can be quickly provisioned and released with little management work or service provider involvement.

1.2 Types of Clouds

There are different types of clouds that can be considered for use depending on the client's needs.

1. Public cloud - a public cloud can be accessed by anyone with an internet connection and access to the cloud space.
2. Private cloud - A private cloud is created for a certain organization or group and restricts access to that group only.
3. Community cloud - Two or more businesses that have comparable cloud needs can share a community cloud.
4. Hybrid cloud - A hybrid cloud is simply a combination of at least two clouds that are a mix of community, private, and/or public clouds.

1.3 Features of Cloud Computing

1. Cloud delivers on-demand resources since it is isolated, therefore there is no requirement for actual sharing.
2. In nature, it is diverse.
3. It also includes data and physical infrastructure in virtualization.
4. It deals with end-user security
5. Clouds are easily usable hiding the deployment details from the user.

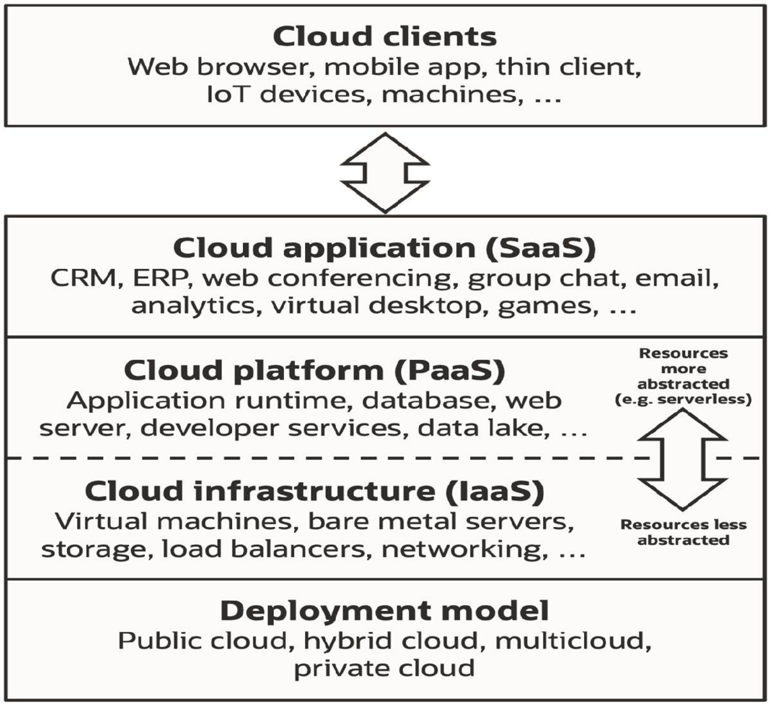
DOI: 10.48175/568

6. Cloud users are typically invoiced on a per-use basis. Advanced payment models and SLA enforcement in a federated Cloud are just getting started, and they're already tearing down one of the biggest barriers to migrating traditional applications to the Cloud.
7. Clouds also disclose a limited number of features (i.e. they offer the user a higher level of abstraction). When compared to the CERN data Grid, for example, Amazon's Simple Storage Service can be considered a limited data Grid.

1.4 Different Cloud Service Providers

Each cloud service provides you with specific functions which give clients control over the cloud depending on the type of provider that has been chosen. Three different categories of cloud service providers exist:

1. Software as a Service (SaaS) - a SaaS provider gives Clients access to both resources and applications. SaaS makes it unnecessary to have a physical copy of the software to install on your devices. By using SaaS, you may access the same program on all of your devices at once, which is more convenient.. In a SaaS agreement, the client has the least control over the cloud.
2. Platform as a service (PaaS) - A PaaS arrangement moves beyond software as a service setup. A PaaS supplier gives customers access to the parts they need to create and run web applications.
3. Infrastructure as a service (IaaS) - The IaaS agreement largely deals with computing infrastructure, as the name implies. The subscriber totally outsources the storage and resources, including the hardware and software, they require under an IaaS arrangement.


Cloud clients
Web browser, mobile app, thin client, IoT devices, machines, ...
Cloud application (SaaS)
CRM, ERP, web conferencing, group chat, email, analytics, virtual desktop, games, ...
Cloud platform (PaaS)
Application runtime, database, web server, developer services, data lake, ...
Resources more abstracted (e.g. serverless)
Cloud infrastructure (IaaS)
Virtual machines, bare metal servers, storage, load balancers, networking, ...
Resources less abstracted
Deployment model
Public cloud, hybrid cloud, multicloud, private cloud

II. IMPACT OF CLOUD COMPUTING ON IT INDUSTRY

Cloud computing has a favorable impact on businesses since it improves income and assists them in achieving their objectives. Rather than constructing their own infrastructure, organizations intend to leverage the cloud's services. The following are some of the privileges of cloud computing technologies that encourage businesses to shift from on-premises infrastructure to the cloud.

- **Unlimited scalability**: The ability of the client to scale up or down in response to the needs of the company is one of the cloud computing's key benefits.. Businesses do not need to worry about upcoming demands because they may easily purchase additional services at any time. Furthermore, as a company expands over time, the cloud can easily scale to meet the additional demand.

- **Efficiency:** Cloud computing makes it easy to consume and set up all of the services without having to worry about resource management or other issues associated with infrastructure setup and administration.
- **Privacy and Security**: Despite the presence of encryption and access-control software, cloud computing allows customers to add additional capacity, more services, and seamless software patching.
- **Flexibility**: Clients can "outsource" aspects of the infrastructure while keeping private data on their own site to some extent.
- **Support for the investigation**: Because logs and data for numerous clients may be co-located and scattered over an ever-changing collection of hosts and data centers, cloud technology services are challenging to analyze.
- **Restoration**: It is very essential to recover the data when some problem occurs and creates failure. The main question that arises here is whether cloud providers can restore data completely or not, this issue can cause a stalemate in security.
- **Advancement of business processes**: Cloud computing and storage access allows clients to access data when they need it. The burden between the processor and the server is significantly reduced, allowing for effective resource management.

III. STUDY OF SECURITY OF CLOUD COMPUTING IN THE IT INDUSTRY

A combination of rules, controls, procedures, and technologies that operate together to safeguard cloud-based systems, data, and infrastructure is known as cloud computing security. In addition to establishing authentication guidelines for certain users and devices, these security measures are customized to safeguard cloud data, support regulatory compliance, and protect customers' privacy. Cloud security can be tailored to the precise requirements of the company, from verifying access to filtering traffic. Additionally, because these rules can be set up and administered in a single location, administration costs are cut, freeing up IT staff to concentrate on other aspects of the business.

The way that cloud security is delivered will be decided by the cloud provider or the installed cloud security solutions. However, the business owner and the solution provider should share responsibilities for implementing cloud security procedures.

- **Security of Computer Systems**: The capacity of a system to protect itself from external threats is referred to as security (Deliberate or accidental). Secured systems are dependable and ready when needed, making them trustworthy. Secured systems that perform as intended without failures or delays assist the industry business which is accomplishing its goals.
- **Data Security**: When properly implemented, robust data security strategies will protect an organization’s information assets against cybercriminal activities, but they also guard against insider threats and human error, which remains among the leading causes of data breaches today. Implementing tools and technology that improve the organization's visibility into where its crucial data is located and how it is used is a key component of data security. In a perfect world, these technologies would be able to automate reporting, apply protections like encryption, data masking, and redaction of sensitive files, and apply protections like encryption, data masking, and compliance with regulatory standards.
- **Information Privacy:** Individuals' desire to control or have some influence over data about themselves is referred to as information privacy. Because the majority of communication methods are now digital, such as mobile phones and the internet, personal communication and personal data privacy have been integrated into information privacy.
- **Damaged Security Infrastructure in cloud computing**: Due to the large volume of data traveling between enterprises and cloud service providers, there is a risk of sensitive data being accidentally or maliciously leaked to untrustworthy third parties. The majority of cloud service data breaches are caused by human mistakes, insider threats, malware, weak credentials, and criminal behavior. Malicious actors, especially state-sponsored hackers, try to take advantage of cloud service security flaws to steal data from the target organization's network for profit or other illegal objectives.

The characteristics that make cloud services easy to use for employees and IT systems also make it harder for businesses to prevent unwanted access. The spread of cloud computing and the reduction in on-premise data centers has not been delayed by the security issues posed by cloud services. As a result, businesses of all sizes must reconsider their network security methods to avoid unwanted data transfers, service outages, and reputational harm.

Authentication and public APIs are new security vulnerabilities that cloud services subject enterprises to. Hackers with advanced skills utilize their knowledge to get access to cloud systems. To sustain a long-term presence on the victim organization's network, hackers use social engineering, account takeover, lateral movement, and detection evasion strategies, typically leveraging cloud service built-in capabilities. Their objective is to move sensitive data to systems under their control.

- **Insider Threats:** Internal representatives are having access to systems and data, as well as cloud service providers' administrators, are examples of insider threats (CSPs). When you sign up for CSP services, you're basically entrusting your data and workloads to a team of people who are responsible for maintaining the CSP architecture.
- **Data Ease of access:** Another thing to consider is whether or not government entities have access to data. Security experts are focusing more on the rules, legislation, and real-world cases that demonstrate whether the government may access data in a private or public cloud via court orders or other means.
- **DoS Attacks:** DoS attacks are now a prominent issue. DDoS assaults often involve flooding a system with requests until it fails. Security perimeters can thwart these attacks by using network compliance rules to keep out repeated requests. CSPs might transfer workloads and traffic to other resources while trying to restore the system. Permanent DoS attacks are more dangerous since they typically corrupt the server's firmware, leaving it unbootable. A specialist will need to manually reload the firmware and rebuild the system from the ground up in this circumstance, which might take days or weeks**.**
- **Direct-access attacks**: Unauthorized users who get physical access to a computer are likely to be able to copy data straight from it. They might also jeopardize security by tampering with operating systems, installing software worms, keyloggers, and covert listening devices, or utilizing wireless mice. Unauthorized access may result in the construction of vulnerabilities in key systems and data manipulation, resulting in frequent data leakages and the loss of private information (personal or financial).
- **Access to Public Cloud Products:** The level of interactivity that customers have over public cloud solutions affects their capacity to evaluate them. From the customer's perspective, users are cautious about moving critical workloads to the public cloud. Big cloud providers, on the other hand, are frequently significantly better equipped and knowledgeable about cloud security than the average private cloud customer. Customers find it reassuring to have total control over their most sensitive data, even if their security technologies aren't very advanced.
- **Cloud-connected Edge Systems:** The cloud edge can refer to edge systems that are connected to the cloud, but it can also refer to server architecture that isn't directly managed by the CSP. Global CSPs rely on partners to deliver services to smaller, geographically isolated, or rural locations since they are unable to create and manage infrastructure in every corner of the globe. As a result, many CSPs lack total control over hardware monitoring and physical box integrity, as well as physical attack countermeasures such as turning off USB port access**.**
- **Man – In – The - Middle (MITM)**: Information of the user can be stolen when the transaction is in process and the same information can be used to perform a financial transaction (Theft) later.
- **Man – In – The-Browser (MITB)**: Information of the user is captured from a website using a fake form and the same information is used to create new accounts and financial transactions to steal money.
- **Man – In – The-PC Attack (MITPC):** In this, weaknesses of the hardware are exploited to secure OTP which may be used to perform financial transactions.

IV. FUTURE OF CLOUD COMPUTING CONCERNING THE IT INDUSTRY

By the end of 2019, 69 percent of businesses, according to 451 research, would have multi-cloud/hybrid IT setups. However, more options result in more challenges. According to predictions, the market will increasingly focus on hybrid and multi-cloud methods in the next few years. For certain businesses, a complete cloud shift is difficult. In contrast, a multi-cloud approach will allow businesses to host all less important tasks with a public cloud provider and use their own

DOI: 10.48175/568

on-premises dedicated servers (or private clouds) to store sensitive data. A hybrid cloud solution, on the other hand, works on a similar principle by dividing data storage between private and public clouds.

Additionally, many professionals thought that individuals living in technologically advanced areas would have access to very sophisticated and expensive local networks that would allow them to have the cloud in their homes. Some people claimed that everything was connected to the internet and that practically all things had unique IP addresses that could be used to connect them to people today.

1. Integration of cloud computing, Big data, AI, and machine learning to boost the market

The increasing adoption of big data, artificial intelligence (AI), machine learning (ML), and others are expected to drive the market's growth. These technologies alter the market environment by enabling users to monitor, analyze, and visualize raw data. Enterprise-wide adoption of AI and ML technologies has simplified data storage issues and empowered data usage. Additionally, these technologies improve decision-making processes, lower operating expenses for businesses, and boost productivity in the commercial sector. Thus, the increasing adoption of big data, AI, and ML is expected to drive the market's growth.Vertex Al, a machine learning platform that aids businesses in maintaining and deploying artificial intelligence (AI) models, was introduced by Google Cloud in May 2021. This aspect would also contribute to the effective management and construction of machine learning projects throughout the course of the whole development lifecycle.

2. Serverless cloud Computing

There are benefits to the serverless paradigm for both users and service providers. A cloud developer no longer has to install and manage servers, virtual machines, or containers as the fundamental computational building block for providing distributed services from the consumer's point of view. Instead, the business logic is highlighted by specifying a collection of functions whose combination results in the desired application behavior.

Stateless programming allows the service provider more control over the software stack, enabling them to, among other things, more transparently distribute security fixes and enhance the platform.

3. Increasing demand for data privacy and cloud migration

The General Data Protection Regulation of the European Union is being increasingly adopted by other nations (GDPR). Independent data security and governance technologies will eventually become a critical component of mission-critical systems. In order to assure the ethical usage and accessibility of cloud data, chief information officers (CIOs), chief information security officers (CISOs), and chief data officers (CDOs) will need to address data governance more and more as of 2021. Increased regulation of personally identifiable information (PII) data will be mandated by regulatory laws in the future to protect consumer privacy.

4. Cloud Data Warehouse Automation

There are a variety of well-known cloud-based data warehouse platforms available, including Amazon Redshift, Google BigQuery, Microsoft Azure, Snowflake, and others, and there are just as many crucial factors to take into account when choosing the best option for your business. Even while many of the widely used cloud data platforms provide comparable functionality, there are significant variances in terms of pricing, scalability, architecture, security features, performance, and other aspects. To accelerate the availability of your analytics-ready data, certain contemporary data integration tools automate the full data warehouse lifecycle. Additionally, a model-driven methodology can assist your data engineers in creating, deploying, managing, and cataloging purpose-built cloud data warehouses more quickly than with conventional methods.

V. CONCLUSION

The next significant development in computing is cloud computing. We gained a basic overview of cloud computing, its categories, and its effects on the IT sector in this article Along with that we have learned about the security of Cloud computing & its future trends. Cloud computing infrastructures are cutting-edge platforms that can be incredibly beneficial to businesses of all sizes. Utilizing resources more effectively thanks to cloud computing enhances profitability.

DOI: 10.48175/568

By just providing the necessary resources during the time they are needed, costs can be reduced. We believe this page has provided answers to most of such queries. We anticipate that this article has addressed many of those queries. With the unprecedented challenges of the COVID-19 pandemic, reports show that a percentage of IT budget allocation goes to cloud technology spending. Companies took the risk of implementing a cloud-based solution to solve the challenges brought by the pandemic, i.e., remote work setup, cloud-enabled workflow, digital conferencing platforms, etc. This article also concentrated on the next trends in cloud computing, which will provide readers with a clearer picture of what's to come in this area.

REFERENCES

[1]. Past, present, and future of cloud computing: an innovation case study by: Garcia, Gene Joseph, V.

[2]. https://www.fortunebusinessinsights.com/cloud-computing-market-102697

[3]. Implementation of Cloud Computing on Web Application – by Liladhar R. Rewatkar & Ujwal A. Lanjewar

[4]. https://www.researchgate.net/publication/322092289_Serverless_Computing_Current_Trends_and_Open_Problems

[5]. https://www.guru99.com/data-warehousing.html

DOI: 10.48175/568