International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2019): 7.583

Cloud Computing: Issues and Challenges

Daharatu Musa Abbas

Abstract: ***With the rise of cloud computing, a batch of new security issues emerges. Users are finding it difficult to transition to Cloud Computing services due to security concerns. According to many studies of prospective cloud adopters, security is the biggest barrier to adoption. The context and service model of cloud computing are discussed in this paper. In addition, a few security concerns and problems are addressed.***

Keywords: Cloud computing, Security issue, Challenges

1. Literature Review

The word "cloud" originates in the world of clouds. Telecommunications as manufacturers started using Virtual Private Network (VPN) for data communication services. Cloud computing deals with applications for computing, software, data access and storage that do not require end-user awareness of the physical location and functionality of the device that offers the services. A current IT trend is cloud computing It moves computing and data from desktops and portable PCs. to large data centres from desktops and portable PCs.

Cloud computing has been a critical piece of suggestions; nowadays, as a result of the opportunities it gives to the environment that is fairly connected. In addition to one solution, cloud computing has expedited suggestions; from adding the in-depth resources to upscaling and downscaling to transition about in-depth properties of the suggestions, no matter what intent is necessary. The cloud computing industry has developed rapidly over the years and is assured of developing at a much faster speed. The versatility it proposes as an associate degree support, such as infrastructure, is one different reason for the achievement of cloud computing.(Sutradhar et al., 2021)

In 2017 Singh & Chatterjee,wrote a paper titled Cloud security issues and challenges. This paper addressed the fundamentals of cloud computing, as well as security concerns, risks, and solutions. In addition, the paper addresses a range of critical facets of cloud computing, including the cloud infrastructure structure, service and implementation model, cloud architectures, cloud protection principles, risks, and attacks. that with the help of a vast volume of virtual storage, cloud computing delivers on-demand facilities over the Internet. The key features of cloud computing are that no costly computing system is set up by the customer and the expense of the resources is smaller. Cloud computing has merged with the enterprise and many other sectors in recent years, the researchers were urged to study new similar developments.

In 2021 Sutradhar et al., explain in their paper that Cloud computing has been a critical piece of suggestions; nowadays, as a result of the opportunities it gives to the environment that is fairly connected. In addition to one solution, cloud computing has expedited suggestions; from adding the in-depth resources to upscaling and downscaling to transition about in-depth properties of the suggestions, no matter what intent is necessary. The cloud computing industry has developed rapidly over the years and is assured of developing at a much faster speed. The versatility it proposes as an associate degree support, such as infrastructure, is one different reason for the achievement of cloud computing.

In 2015, S. Khan et al. have discussed in their paper that Cloud computing has the ability to deliver cost-effective, easy-to-manage, scalable, and efficient services on-demand over the Internet. Cloud computing expands the capacities of hardware services by maximizing and sharing their use. The features mentioned above allow businesses and individuals to move their apps and resources to the cloud. Also, vital infrastructure, such as power plants and transport networks, is moving to the cloud computing model. Third-party cloud service providers, on the other hand, present potential security risks. In a shared network where many users are collocated, the transfer of user properties (data, programs, etc.) outside of administrative control raises security issues. This study examines the security problems that exist as a result of cloud computing inherent existence.

In 2010, the authors of this essay address the protection and privacy problems that are caused by the peculiar features of clouds, as well as how they are linked to different distribution and implementation models. They explore different approaches to solving these issues, as well as existing technologies and possible work that will be necessary to establish a stable cloud storage environment.(takabi et al.)

In 2015 the authors of this paper intend to explain the existing open problems and concerns of Cloud computing in this article. The paper was broken down into three sections: first, we looked at the cloud computing infrastructure and the various services it provided. Second, focusing on the service layer, we illustrate many security challenges in cloud computing. Then, from the viewpoint of Cloud computing implementation, they recognize some open problems as well as their potential consequences. Finally, they illustrate the platforms available for cloud research and development in the present century. (S.Mishra et al.).

In 2010, the authors of this paper provide a survey of cloud computing, outlining core ideas, design standards, current deployment, and analysis challenges. The aim of this paper is to provide a deeper understanding of cloud computing architecture issues and to recognize relevant research directions in this rapidly growing field. (Q.zhang et al.)

Purpose

The purpose of this paper is to research on security issues and challenges of today's Cloud Computing services.

2. Aim and Objective

With the rise of cloud computing, several of these new security issues emerge. Users are finding it difficult to transition to Cloud Computing because of security concerns. According to many reports of potential cloud adopters, protection is the biggest barrier to adoption. The background and service model of cloud computing are discussed in this paper. In addition, a few security problems and threats are also discussed.

3. Introduction

Cloud Computing

Definition

Cloud computing (CC) is the distribution of computing resources such as servers, storage, and databases over the internet. On the internet, networking, applications, analytics, and information are all available. This is a broad term that includes a wide variety of hardware and software technology. Cloud computing's primary purpose is to allow efficient use of distributed services, merge them to achieve higher efficiency and to address large-scale computation.

Features of Cloud Computing

1) On-demand access: Cloud storage resources can be used if required by customers. For Hadoop data analysis, every consumer data analytics organization, for example, uses an Amazon EMR or EC2 cluster. The user then turns on the cluster when he or she needs it, pays for the time span he or she has used, and then terminates the cluster when his or her job is finished.
2) Pricing is reasonable:
In the case of certain services and networks that we use, cloud storage services are affordable. When we talk about big data, we will see things even more plainly. If an organization has to handle 100 Terabytes of data, the cost of constructing infrastructure and managing it would be greater than if they use cloud storage resources.
3) Acceleration in applications has been simplified:
Cloud storage platforms provide a range of programs that can be accelerated rapidly and efficiently without the use of difficult procedures.
4) Elasticity refers to a cloud's capacity to instantly extend or compact infrastructural services in reaction to a rapid rise or decrease in demand, enabling the workload to be controlled efficiently. This elasticity assists in the elimination of infrastructure costs.
5) Cloud scalability is used to manage increasing workloads under which good output is often needed to work successfully with software or applications.
6) Effective resource allocation: Another essential function that assists in resource allocation performance is efficient resource allocation. If we use multiple instances of cluster for data processing, for example, resources can be shared effectively so that no cpu or memory stays unused for a prolonged period of time.
7) Quality in terms of energy: Cloud hosting systems and networks are energy efficient in the way that they consume less energy if anyone wishes to maintain those servers going 24 hours a day, seven days a week. Upwards
8) Build and use third-party providers with ease: Cloud computing enables the development and usage of third-party applications in a streamlined fashion. For e.g., AWS makes it easy to build EMR Hadoop clusters, so we don't have to put in much effort.
9) Self-service: Self-service is at the centre of cloud computing. The customer should be able to communicate with the cloud to execute activities such as creating, installing, handling, and scheduling. The customer should be able to access computing services when and when they are needed, with no interference from the cloud service provider.

Cloud Computing Service Model

There are three types of service model in cloud comping

1) SOFTWARE AS A SERVICE (SAAS): Business application software is delivered to the customer as on-demand services in Software as a Service (SaaS). Since clients buy and use software components from a number of suppliers, the most critical thing are that the information managed by these composed providers is reliable. GoogleApp, for example, is an example of a SaaS provider.
2) PLATFORM AS A SERVICE (PAAS): PaaS is a cloud-based technology or development tool that helps developers to build their own cloud-based apps. e.g. Microsoft Azure, and Google AppEngine.
3) INFRASTRUCTURE AS A SERVICE (IAAS): Iaas refers to the delivery of computer hardware as a service, such as servers, networking infrastructure, storage, and data centre space. That may also require the provision of operating systems and virtualization technologies for resource management.

Cloud Deployment Model

To allow fast loading, most cloud hubs have tens of thousands of servers and storage devices. It's popular to be able to pick a geographic area to get data "closer" to consumers. As a result, cloud infrastructure implementation models are classified according to their geographical position.

1) **Private Cloud:** It is a cloud-based infrastructure that is used by small companies. It allows you more access power. Internally, the data is backed up by a firewall, and it can be hosted either internally or externally. Private clouds are suitable for companies with strict security, management, and availability criteria.
2) **Public Cloud:** This form of cloud infrastructure is made available to the general public over a network. Customers have no choice about where the infrastructure is situated. Which is based on a cost-sharing model for all consumers, or it may be in the form of a licensing scheme, such as pay-per-use. Public cloud implementation models are suitable for companies with changing and rising demands.

3) **Community Cloud:** It is a model that is shared by organisations that are part of a specific culture, such as banks, government departments, or commercial enterprises. Members of the group typically have common questions regarding anonymity, efficiency, and protection. This cloud infrastructure implementation model is managed and hosted either internally or by a third-party provider.
4) **Hybrid Cloud:** This model blends the best aspects of both private and public clouds, but each can function separately. Furthermore, internal or external vendors may provide services as part of this cloud infrastructure implementation model. Scalability, stability, and protection are all benefits of a hybrid cloud.

Cloud-Computing Security Issues

Security issues related to SAAS

- Inability to see what data is contained in cloud systems
- Malicious actor exploits data from a cloud program
- Inability to track data in transit to and from cloud applications.
- Insufficient control of who should access confidential data.

Since most shared security management models leave those two as the primary responsibility of SaaS users, SaaS cloud security issues inevitably revolve around data and access. Any enterprise must know what data they hold in the cloud, who has access to it, and what type of security they (and the cloud provider) have introduced.

Security issues related to PAAS

- Workloads and accounts in the cloud are being developed without the knowledge of IT.
- Total lack of control over who has access to classified information.
- There aren't enough people with the right expertise to protect cloud assets.
- There is no means of telling what data is in the cloud.
- Inability to avoid data theft or abuse by malicious insiders
- Cloud computing is vulnerable to sophisticated risks and assaults.

In IaaS, data protection is essential. Additional threats arise as user liability expands to software, network traffic, and operating systems. As the core of IaaS risk, organizations should recognize the recent evolution of attacks that spread beyond results.

It's important to determine the ability to prevent fraud and monitor access while designing cloud infrastructure. Determining who has access to data in the cloud, tracking resource modifications to detect abnormal behaviour, securing and adding network analysis of both north–south and east–west traffic as a potential signal of compromise are all quickly becoming standard measures in protecting large-scale cloud infrastructure deployments.

4. Issues and Challenges of Cloud Computing

1) Security and Privacy

The three most pressing concerns of cloud adoption are security, efficiency, and availability. The key concern is addressing security and privacy problems that arise as a result of data and device transfer through networks, data leakage, heterogeneous resource nature, and multiple security policies. Data collected, processed, and moved outside of an organization's reach poses an underlying danger, leaving it vulnerable to a variety of attacks. Cloud storage raises privacy issues because internet providers can have access to data on the cloud, which may be modified or otherwise deleted by mistake or on purpose, resulting in significant business trust and legal implications.

2) Performance

The second most important problem in cloud adoption is performance. When a customer switches to cloud computing technology, the cloud would have better performance. The features of software operating on the cloud infrastructure are commonly used to assess performance. A lack of appropriate resources will lead to poor results. small disk space, bandwidth, CPU speed, memory connections to the internet.

3) Availability and Reliability

The degree of reliability and availability of any technology determines its power. The term "reliability" refers to how often services are available without interruption (data loss) and how often they fail. Downtime is one of the most significant factors that contributes to cloud computing's unreliability. The use of backup resources is one way to ensure reliability.

4) Resource Management and Scheduling

Resource provisioning is the process of allocating and managing capital in order to provide the optimal quality of operation. Job scheduling is a form of resource provisioning in which the order in which jobs are executed is determined in order to complete job execution and maximize those parameters. Turnaround time, reaction time, waiting time, throughput, and resource usage are also important factors to consider. The partitioning of jobs into parallel assignments, the interconnection network between clouds or processors, the assignment of priority to jobs, and the selection of jobs are the main issues of job scheduling on cloud networks.

Job stability, extent of pre-emption assisted, workload characteristics, memory allocation, mission execution control, resource allocation, and so on. Job scheduling is a crucial factor that must be carefully considered; a poor scheduling approach may have a disastrous impact on efficiency, resulting in resource waste and a failure to meet Quality of Service (QoS) requirements.

5. Conclusion

In the near future, cloud computing will be an important part of nearly all industries and it is expected to transform the IT sector. It is built on a pay-as-you-go model for providing services over the internet, with benefits such as no upfront costs, less IT workers, and reduced operational costs, to name a few. While cloud infrastructure has promising futures for both businesses and academics, a number of challenging problems, such as security, efficiency, usability, scalability, interoperability, and virtualization, must be carefully approached. Improvements in bandwidth infrastructure, corresponding service models, and security models have the potential to completely transform this sector, as well as the IT industry. This paper has explored the nature of cloud computing and shed some light on some of the problems and concerns that must be tackled in order to understand the cloud's adoption and make it a dominant part of our lives in order for us to succeed.

References

[1] Dillon, T., Wu, C., & Chang, E. (2010). Cloud computing: Issues and challenges. *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*. https://doi.org/10.1109/AINA.2010.187

[2] Sutradhar, N., Sharma, M. K., & Sai Krishna, G. (2021). Cloud Computing: Security Issues and Challenges. *Lecture Notes in Electrical Engineering*. https://doi.org/10.1007/978-981-15-7486-3_4

[3] Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. In *Journal of Network and Computer Applications*. https://doi.org/10.1016/j.jnca.2016.11.027

[4] Sutradhar, N., Sharma, M. K., & Sai Krishna, G. (2021). Cloud Computing: Security Issues and Challenges. *Lecture Notes in Electrical Engineering*. https://doi.org/10.1007/978-981-15-7486-3_4

[5] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2010.12.006

[6] Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*. https://doi.org/10.1016/j.ins.2015.01.025