WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cloud Security

Sagar L. Sonawane, Priyanka S. Wagh

ASM'sInstitute of Management & Computer StudiesMCA Institute
Affiliated to University of Mumbai & Approved by AICTE, C-4, Wagle Industrial Estate, Near Mulund Check Naka,Opp. to Aplab, Thane (W) – 400604.

ABSTRACT:

Cloud Computing is increasingly becoming popular as many enterprise applications and data are moving into cloud platforms. However, a major barrier for cloud adoption is real and perceived lack of security. In this paper, we take a holistic view of cloud computing security - spanning across the possible issues and vulnerabilities connected with virtualization infrastructure, software platform, identity management and access control, data integrity, confidentiality and privacy, physical and process security aspects and legal compliance in cloud. Cloud Computing is not considered as application oriented but service oriented. A major concern in adaptation of cloud for data is security and privacy It is very important for the cloud service to ensure the data integrity, privacy and protection. For this purpose, several service providers are using different policies and mechanism that depend upon the nature, type and size of data.

Keywords : Cloud computing security, Firewall, Data security.

Introduction :

Cloud security, also known as cloud computing security, is the practice of protecting cloud-based data, applications and infrastructure from cyber attacks and cyber threats.

Cloud computing security is an emerging field in computer security, designed to protect data and information within the infrastructure of cloud computing, which involved remotely networked servers. Cloud computing is proving to be a popular form of data storage. Rather than taking up space on a hard drive, photographs, documents, and other data can be stored in the "cloud."

RISKS AND SECURITY CONCERNS IN CLOUD COMPUTING:

Several risks and security concerns are associated with cloud computing and its data. However, this study will discuss about the virtualization, storage in publiccloud and multitenancy which are related to the data security in cloud computing.

Virtualization :

Is a technique in which a fully functional operating system image is captured in another operating system to utilize the resources of the real operating system fully. A special function called hypervisor is required to run a guest operating system as a virtual machine in a host operating system. Virtualization is a foundational element of cloud computing which helps in delivering the core valuesof cloud computing. A solution to above mentioned issues is a better planning for the use of virtualization. Resources should be carefully used and data must be properly authenticated before de-allocating the resources.

Storing data in a public cloud :

Is another security concern in cloud computing. Normally clouds implement centralized storage facilities, which can be an appealing target for hackers. Storage resources are complicated systems that are combination of hardware and software implementations and can cause exposure of data if a slight breach occurs in the public cloud.

In order to avoid such risks, it is always recommended to have a private cloud if possible for extremely sensitive data.

Multienancy:

Shared access or multitenancy is also considered as one of the major risks to data in cloud computing . Since multiple users are using the same shared computing resources like CPU, Storage and memory etc. it is threat to not only a single user but multiple users. In such scenarios there is always a risk of private data accidentally leaking to other users.

These types of issues can be taken care of by wisely authenticating the users before they can have access to the data. Several authentication techniques are in use to avoid multitenancy issues in cloud computing

Data at Rest:

Data at rest refers to data in cloud, or any data that can be accessed using Internet. This includes backup data as well as live data. As mentioned earlier, sometimes it is very difficult for organizations to protect data at rest if they are not maintaining a private cloud since they do not have physical control over the data. However, this issue can be resolved by maintaining a private cloud with carefully controlled access.

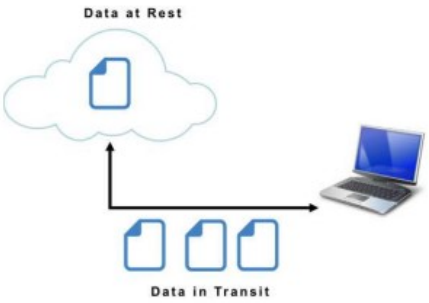

Fig 1: Data at Rest and in Transit.

Advantages :

One of the advantages of Cloud Computing is that data can be shared among various organizations. However, this advantage itself poses a risk to data. In order to avoid potential risk to the data, it is necessary to protect data repositories. One of the key questions while using cloud for storing data is whether to use a third party cloud service or create an internal organizational cloud. Sometimes, the data is too sensitive to be stored on a public cloud, for example, national security data or highly confidential future product details etc. However, in a post-COVID world, cloud technology has become a necessity, and cloud security is a critical concern.Almost overnight, businesses of all sizes needed to accommodate an abrupt shift to remote work. It was cloud technology that helped achieve this goal, enabling businesses of all sizes to operate remotely. In addition, it has become necessary to scale up digital operations and accelerate digital transformation. These digital capabilities enabled consumers to access services remotely, and employees to work remotely at an unprecedented scale.Remote access paradigms, enabled by cloud technology, have become critical to ensure business continuity in the pandemic. Unfortunately, this has made cloud infrastructure a primary target for attackers.

CONCLUSION:

Increased use of cloud computing for storing data is certainly increasing the trend of improving the ways of storing data in the cloud. Data available in the cloud can be at risk if not protected in a rightful manner. This paper discussed the risks and security threats to data in the cloud and given an overview of three types of security concerns. Virtualization is examined to find out the threats caused by the hypervisor. Similarly, threats caused by Public cloud and multitenancy have been discussed. Data in different states has been discussed along with the techniques which are efficient for encrypting the data in the cloud.

REFERENCES :

1. https://www.researchgate.net/publication/259764167_The_Research_and_Design_of_Cloud_Computing_Security_Framework
2. https://www.engpaper.com/cloud-computing-security-2019.htm
3. https://www.papermasters.com/cloud-computing-security.html
4. http://www.tjprc.org/publishpapers/2-14-1375100443-33.%20Recent%20advances.full.pdf