IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

Overview of Cloud Security

Jasline Sharon Tauro[1], K Isha Hegde[2], Khatheeja Safreena[3], Krishnitha[4]
Students, Computer Science and Engineering[1,2,3,4],
Alva's Institute of Engineering and Technology, Mijar, Mangalore, Karnataka
jaslinetauro10@gmail.com[1], ishahegde50@gmail.com[2],
khadhijashafreena15@gmail.com[3],krishnithashetty@gmail.com[4]

Abstract: *Cloud computing is defined to compute or process the data that is stored in a particular cloud. This cloud has several layers, each layer meant for its unique functionality and computes the data based on the same functionalities, and based on those functionalities it has certain risks. When we store any amount of data in a particular cloud there will be certain security threats and storage aspects and controversies based on which particular type of cloud deployment models, we choose to store the data. Also, the various kinds of security techniques that we can implement to resolve those threats of security and storage challenges.*

Keywords: Cloud Computing, layers of cloud, Functionalities, Cloud Storage

I. INTRODUCTION

During the execution of cloud innovation, information security is one of the main pressing issues that was being faced. Nearly, all the organizations working on cloud technology are still dreading the challenges to secure the data. All the association needs to make something similar to security boundaries as they are now utilizing with their inward information/assets. It is compulsory to comprehend and observe the information insurance challenges before re-evaluating the information security in distributed computing. Distributed computing addresses numerous particular worries and challenges with the security of the information. While utilizing cloud processing for putting away the information, one needs to pick or find an outsider supplier and, requirements web to get to the information. Consequently, we can say information permeability and information control are restricted while utilizing distributed computing. Utilizing of cloud empowered innovation likewise raises the issue of how information could be secure. Information storage in cloud space is a higher priority than the computer. The physical storage is at a misfortune due to the cost related and an assortment of different variables. Many organizations have grown a quick and reasonable foundation to resolve the issue of information assortments and availability to clients worldwide. However, all distributed storage is powerless against an infringement of security mechanism, which poses a threat especially when a client stores confidential data on the cloud.

II. ARCHITECTURAL COMPONENTS

Cloud computing is not a single piece of technology like a microchip or a cell phone. Rather, it's a system primarily comprised of three services: software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS).

2.1 Software-as-a-Service (SaaS)

The SaaS is the main layer of distributed computing. It is moreover known as the association layer of cloud computing. The clients can make an association with the cloud through this layer. This layer offers every one of the utilizations of the cloud on a shared premise. For the most part, the Internet can be used to associate SaaS with different layers of the cloud [1]. Administrations alongside programming for working contraption, data sets, servers, network get passage to, energy, and records focus space, etc. are contracted via the Cloud supplier [4].

2.2. Infrastructure-as-a-Service (IaaS)

The center layer of distributed computing has a place with PaaS. This layer can likewise be utilized to associate the SaaS and IaaS layer of a cloud [1]. The PaaS layer is extraordinarily intended for developers or for experts who are liable for planning and creating of utilizations [1] PAAS offers a layer of utilization development or an environmental element to

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

grow programming which is epitomized and introduced as assistance [5]. All the applications utilized at the SaaS layer are planned at the PaaS layer. It has applications like working framework, programming dialects, and so forth, which are expected for fostering an application.[1]

2.3 Platform-as-a-Service (PaaS)

This is the establishment layer of a cloud. It has all the equipment assets which are expected for fostering an application.[5] It offers assets like servers, stockpiling plates, and any remaining equipment according to the necessities including all the organizing tools [1]. IAAS determines the dispersion of registering assets, fundamental capacity, and processing abilities for executing administrations utilizing virtualization innovation.[1] IAAS gives key processing assets like servers, stockpiling framework, organization, and so on [1]

III. Different Cloud Deployment Models

3.1 Public Cloud

The public cloud is in general utilized by the customers and is available to the public. consequently, on every occasion a type of garage is utilized by the public then it comes beneath the public cloud [5]. As an instance, Google force comes underneath the form of public cloud wherein public uses the storage receives a positive quantity of garage area and that they could get admission to it whenever and everywhere [4]. it is a very secure manner and everyone login it the usage of exceptional emails and passwords. there are many dangers and advantages to the usage of Cloud Computing [4][5].

3.2 Private Cloud

Private Cloud is frequently when an organization wishes storage. it's far committed storage [5]. So, the foremost distinction among the public and private cloud is that in the public cloud many customers can percentage the storage but in a private cloud, the most effective unbiased organization they have got devoted storage [4].

3.3 Hybrid Cloud

Hybrid cloud is whilst any company uses non-public cloud plus public cloud is referred to as hybrid cloud [5]. As an instance, if one academy wants to shop all of its valuable videos to devoted storage then it would come below the non-public cloud and the academy also replies to the pupil the use of e-mail, so e-mail is nothing but is an example of public cloud. So, this situation fits for hybrid cloud [4]. Salvi et al proved network cloud as when many companies which include one concept that we could buy one garage and allows try to divide the part of the garage for us. as an example, count on there are three corporations that can be sharing the garage between them then that is known as the network cloud [4][5].

3.4 Community Cloud

This sort of model is utilized at an association level. It is utilized by a specific local area like a particular government division, bank, and so on This sort of model is utilized to give explicit administrations to its client through a local area [1].

IV. Security Challenges In Cloud Computing

- **Access Control and Data Stealing:** Nowadays, the data that is stored in the cloud has become so accessible that all unauthorized users are stealing or corrupting the data by using various methodologies like hacking using attacks like DNS server attacks, Man in the middle attacks, phishing, conducting scams, or hijacking the data so that the authorized users cannot make use of it. Those unauthorized users can convert this data as malicious.
- **Data Control:** Another threat of data in cloud security is data control and leakage like access control. The data also gets corrupted by some authorized insiders like employees or hosts [4]. As they know the exact functioning of data inside the cloud, they use some security mechanisms to get the data and corrupt it [5]. Also, some ex-employees use certain techniques to perform encryption and decryption of the data. The estimated percentage of data leakage in the cloud is around 64% [1].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

- **Data Location:** The cloud is a very large platform that stores a very huge amount of data. The data that is located in one particular file is very difficult to locate also, it is very difficult to know the particular data is stored in which datafile or database [3].
- **Data Backup:** As we know the data in the cloud can be taken by theft. So, there must be a certain data backup plan or method where all the duplicate data resides. So, when the original data is leaked the authorized user can access the data and do the task. Even if there is some certain backup process the data control problem reoccurs.

V. Security Issues In Cloud Layers

5.1 SaaS (Software as a Service) Layer

As this is the topmost layer of the cloud, here the user and server interactions take place hence the security issues like data leakage, malware attacks or hijacking will be more [6]. It also has security concerns like lack of technological knowledge among cloud employees [2].

5.2 PaaS (Platform as a Service) Layer

This is the middle layer of the cloud, and this layer is used as an interactive layer between SaaS and IaaS. Here it has security issues like application functioning, storage issues, network issues in the cloud that might have security breaches [2][6].

5.3 Infrastructure-as-a-Service (IaaS) Layer

This is the third layer of cloud computing, it includes different security concerns like no proper interaction, lack of work distribution and understanding, data sensitivity, and attacks [6]. It also includes issues such as information security, as the users can add or store their data which can result in, multiple redundant data availability which is very difficult to know where and how it is stored [2].

VI. Cloud Storage Issues

With the rising pace and accessibility of distributed computing, it's nothing unexpected that companies have committed. A cloud server is a flexible apparatus that meets capacity and interaction necessities, yet in addition assists with saving a great many dollars in IT ventures for organization information. While utilizing organization cloud space and record appropriation frameworks, coming up next are key perils that ought to be recognized.

6.1 Out of Control Data

With cloud items like Google Drive, Dropbox, and Microsoft Azure turning into a typical part of corporate development, associations have needed to manage more contemporary security concerns. The issue here is that when outsiders exploit record-sharing frameworks, the data is generally removed from their organization's IT climate, and that implies that data security is far taken out from the organization's administration.

6.2 Data Overflow

More information and information bases are progressively being put away in the public cloud by the present organizations. The public cloud has made it undeniably more proficient, adaptable, and basic for organizations to embrace innovation. Any organization that has gotten back from the cloud has done as such because of a paranoid fear of information spilling. This tension stems from the way that the cloud is a multi-client framework with appropriated administrations. It's likewise a believed outsider assistance, and that implies the merchant could see or blunder data. The abilities of an outsider must be addressed since they are human. Information spillage can be brought about by an assortment of outer risks, for example, cloud-based hacking or access into cloud client accounts.

6.3 Snooping

Without the choice of hacking security systems set up, cloud information is among the riskiest. Moreover, truth sticks on and is sent through the web, representing a genuine gamble danger, and data can in any case be caught in its excursion.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

Outsiders are unable to access Metadata from the cloud because of the incredible security design, which incorporates encrypted documents transferred over a tightly guarded network.[2].

VII. Data Security Techniques In Cloud Computing

- **Encryption:** Encryption is the process message that can be accessed only by an authorized person. There are different techniques for encryption of data in rest or transit. Cryptographic techniques such as stream cipher, block cipher, the hash function is some of them. In cryptography, a message is encoded by using the encryption key, and by using the decryption key it can be decoded. Hence data can't be accessed even by the cloud vendor unless he has access to the key [8].
- **Access Control:** Access control is a fundamental security component that consists of both authorization and authentication. It is a security technique that avoids security breaches by limiting access to the system and its resources. There are various access control models such as DAC, MAC, RBAC, etc which can be employed in different kinds of cloud environments [10].
- **Virtual Private Network (VPNs):** VPN transmits data securely by connecting private networks and public networks. It protects data in an unsecured network by establishing a private connection using a process called a tunnel. It provides data confidentiality using encryption and a message digest is used to check the data integrity of the data being transmitted [9].
- **Masking:** Masking is also known as data obfuscation, de-identification, or depersonalization [7] is the process of replacing sensitive information with a duplicate. It reduces the threat of disclosing sensitive information. Shuffling, Substitution, Encryption are some of the techniques for data masking.

VIII. Security Controversy In A Cloud Computing System

Cloud computing companies continue to reap the benefits of promises to improve performance, robustness, and agility at a rapid rate. The cloud security review highlights what works and what doesn't for a security team in securing their cloud records, applications, and services under this mutual accountability approach. The findings are a continuation of previous issues.

1. According to cyber-security experts, the highest risk is data retention and leakage of 64 percent.
2. 42 percent improper access detection and misuse by unauthorized access; this year's most widely discussed cloud security risk is ranked first in the study.
3. 42 percent of cloud platforms are misconfigured.
4. Enforcement and infrastructure safety visibility are two of the most difficult defence activities for the SOC team.

With regards to choosing cloud-based security arrangements, huge firms evaluate an assortment of fundamental advantages; respondents might lean toward cost reserve funds and quicker establishment and proficiency over cloud-based security systems. As indicated by the examination advancement is important to further develop the public cloud wellbeing in the structure of a current calculation and model, ongoing issues incorporate significant dangers for information misfortune and spillage.[1]

IX. Benefits Of Using Secured Cloud

We took a gander at the procedures for making information secure in the past segment of the paper. In the accompanying ways, this helps our plan of action.

- Guarding our basic business information against digital assaults.
- It fills in as an impediment to inner security dangers.
- Above all, it prepares for information misfortune.[1]

X. Conclusion

Cloud computing is one of the fastest emerging technologies as all organizations and businesses are storing their data in the cloud. It reduces the cost and time of storing data physically. Security technology is the major strength of cloud computing. It is crucial to store data in the cloud correctly and protect the stored data efficiently. Hence, undeniably surging

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

the trend of upgrading the methods of storing data in the cloud. The presented paper gives an overview of various cloud architectural components and deployment models that all should know before using the cloud. It also discusses different security challenges, security issues in cloud layers, storage issues, and techniques to overcome cloud problems. The presented paper also discusses the merits of using cloud storage systems.

REFERENCES

[1]. Mukesh Joshi, Sandeep Budhani, Naveen Tewari, Satyam Prakash "Analytical Review of Data Security in Cloud Computing" 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM).

[2]. G Nagarajan, Dr K.Sampath Kumar "Security Threats and Challenges in Public Cloud Storage" 2021 International Conference on Advanced Computing and Innovative Technologies in Engineering (ICACITE).

[3]. Monjur Ahmed and Mohammad Ashraf Hossain "Cloud Computing and Security Issues in the Cloud" International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[4]. G.Shanmugasundaram, V.Aswini, G.Suganya "A Comprehensive Review On Cloud Computing Security" 2017 International Conference on Innovations in information Embedded and Communication Systems (ICIIECS).

[5]. Gurmeher Singh, Puri Ravi Tiwary, Shipra Shukla "A Review on Cloud Computing".

[6]. Frederick R. Carlson "Security Analysis of Cloud Computing".

[7]. K.Sharmila, S. Borgia Anne Catherine, Sreeja V.S "A comprehensive Study of Data Masking Techniques on cloud" International Journal of Pure and Applied Mathematics Volume 119 No. 15 2018, 3719-3727.

[8]. Ahmed Albugmi, Madini O. Alassafi, Robert Walters, Gary Wills "Data Security in Cloud Computing" Fifth International Conference on Future Generation Communication Technologies (FGCT 2016).

[9]. M. Judith Bellar "Cloud Computing Security with VPN" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 8, August 2015.

[10]. Iqbalinder Singh Sohal, Amardeep Kaur "Review on advanced access control models in cloud computing" TRJ VOL. 2 ISSUE 4 JULe Y-AUG 2016