IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

An Analysis on Cloud Security and the Function of Data Security Protocols

Gulista Khan, Associate Professor,
College of Computing Sciences and Information Technology, Teerthanker Mahaveer University,
Moradabad, Uttar Pradesh, India
Email Id- gulista.khan@gmail.com

ABSTRACT: ***A variety of services are now available to end users thanks to the development of cloud computing. Due to its advantages, most sectors are now able to leverage the cloud for their applications. Most cloud platforms have security holes and are vulnerable to several attacks. This study reviews the several security protocols that businesses may take, as well as some of the more specialized security procedures including authentication, authorization, encryption, as well as security systems. The processes for each safety measure are also looked at. Giving a basic overview of cloud computing security is the aim of this study. An explanation of cloud computing security, including its definition and scope, is provided. An ecosystem for cloud security is given to demonstrate the capabilities of each industry stakeholder. The security implications of cloud security are then considered for companies and operators. This study will present a new investigator as well as try to highlight the substantial security concerns and issues that emerge in public cloud systems, particularly with regard to data storage, administration, and processing.***

KEYWORDS: ***Cloud Computing, Hybrid Cloud, Public Cloud, Service Providers, Technology, Virtualization.***

1. INTRODUCTION

Grid and grid computing, as well as cloud computing, have advanced with the development of complexity, processing, and storage capacity in the past. The National Institute of Standards and Technology describes cloud computing as a concept that offers a readily available, on-demand pool of programmable computing resources that can be set up fast and simply with little to no assistance from administrators or service providers [1]. Cloud computing has undergone a substantial transition that sets it apart from other cloud applications. Logical processes are increasingly resembling their masculine counterparts as a result of virtualization. The most effective technique to use a multitude of sources is through virtualization. Because of features like scalability, availability, adaptability, multi-tenancy, flexibility, and simplicity of use, cloud computing has emerged as the industry standard [2].

Cloud computing security is a big issue that necessitates attention. Data storage, computing, and safeguarding against dangers including eavesdropping, denial of service assaults, logging security problems, and many more are all covered under cloud security issues. In order to meet the increasing service demand of customers, the cloud must not only provide essential functions while adhering to multiple cloud standards and maintaining the quality of service, but also find answers to a number of security challenges [3]–[5]. Demand for a range of resources, including photos, data, and cloud infrastructure, to be stored in the cloud and accessed and shared via an Internet connection has increased as a result of recent end-user cloud migration. The enterprise's software and business architecture will be totally rethought and rebuilt thanks to cloud computing. In this

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

article, the key cloud computing security concerns are summarized along with recommendations for how to handle them [6].

A huge group of computers that collaborate to do numerous tasks, computations, and other operations are referred to as "cloud computing" As it enables numerous pieces of software or programs to run on a single instance, it is a distributed computing solution. Some advantages of cloud computing include high capacity, reliability, multi-tenancy, dynamic resources, and scalability. Users will be charged for the resources they have used in the cloud, according to the pricing model that underpins it. Cloud service providers are expanding at a 90% yearly pace, according to a recent survey. Cloud technology, for instance, may be broken down into many sorts based on how many services they provide. Technology categories include private cloud, public cloud, hybrid cloud, and infrastructure cloud as a service. The service delivery models can be classified as:

- Infrastructure as a Service (IAAS),
- Software as a service (SAAS), and
- Platform as a Service (PAAS).

The descriptions of each of these models are described below.

1.1. Software as a service (SAAS):

'The idea of "Software as a Service" (SaaS) provides all the software required to carry out various operations while living up to user expectations. Depending on how long they use the application, users will have to pay a charge. The program is generally accessible to everyone on the cloud. A research claims that the "SaaS" platform dominates sales of public clouds. Some of the providers of "SaaS" are Salesforce.com, Google, and Intuit. For example, Intuit provides 256-bit advanced encrypted messages, video monitoring, and incident management among other encryption technologies [7]. There are occasions when Intuit has outages, which has an effect on the level of service. Cost is another problem that has to be solved. The sales force, one of the most creative organizations in the United States, employs cyber security experts to carry out security protocols, vulnerability scanning, third-party verification, and periodic structural evaluations to protect data kept in the cloud. Salesforce is susceptible to fraud attempts, and worries regarding the protection of data stored in the cloud still exist.

1.2. Platform as a Service (PAAS):

People may take advantage of the cloud computing paradigm by using various apps in an expedited but scalable method. The file systems, software, and apps needed to set up a cloud system are all handled by its platform as a client service. Additionally, it aids in the creation of agile applications. Numerous features are available, such as automatic scaling, flexibility, support for various data centers, and the opportunity to choose from a variety of configurations. When moving to the cloud, data management becomes a key issue, and the source must still retain data accessible in the cloud. With security tools including file servers, firewalls, third-party authentication, security threat monitoring, and Secure Shell for secure data transfer, Microsoft is a leader in the field as a service provider [8]–[10]. Hosting data outside of the customer's country might provide problems with data sovereignty, which would have been a major drawback. The 128-bit AES encryption standard,

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

which provides assurance against unauthorized disclosure, is used by Google to guarantee continuous data encryption.

The data is automatically safeguarded when certain entities try to access the saved data as well as read the contents. Among the security features offered by Google are internal audit, Rat Proxy, troubleshooting and administration based on Secure Shell Connection (SSC) cloud lock, and log analysis. The major disadvantage has been that Google used to have a memory limit and was susceptible to outages and service interruptions. Massive volumes of user data may be stored with Amazon-S3 at several storage locations all over the globe. A number of security technologies are available from Amazon, such as Amazon Session Management and Authentication (AASM) as well as Amazon Cloud Watch (ACW) that keeps an eye on Amazon resources and applications. The secure hash algorithm (SHA-1) signatures and hash-based message authentication code (HMAC) are both used for verification in the Amazon Web Services Management Interface. Despite being the biggest and most reliable storage provider, Amazon-S3, the web service for data transmission is slow and inconsistent. If Amazon wants to be a top storage provider, it must concentrate its efforts on finding concerns with maintaining data protection.

1.3. Infrastructure as a Service (IAAS):

According to Margaret Rouse, the idea of "infrastructure as a service" includes a lot of the resources needed for an organization to run efficiently, including hardware, networking tools, storage, and so on. IAAS features include desktop virtualization, policy-based services, utility computing models, and automation of administrative tasks. Among the real-time service providers are Qwest, EMC, and Verizon Terri Mark. Qwest offers a variety of services including Web Defense, PCI Compliant Hosting as well as Contact Center Solutions, Secured IP Gateway, DDoS Mitigation Service, as well as Professional Security Agencies. Other protective measures include firewalls, anti-virus/anti-spam software, compliance audit policy enforcement, processing incoming calls, as well as hosting IVR for backups and preservation.

2. DISCUSSION

2.1. Types of Cloud-based Usage:

Each cloud pools, abstracts, and distributes scalable computing resources along a networking. Cloud computing, which refers to the process of executing workloads inside that system, is also possible with any cloud type. Additionally, each cloud is built using a different combination of technologies, nearly usually including an operating system, a management system, as well as application programming interfaces (APIs). For extra features or greater efficiency, virtualization as well as mechanization technologies may be applied to all types of clouds. There are some cloud based usage are discussed below as well as shown in below Figure 1.

2.1.1. Private Cloud:

A private cloud is developed or assigned to a specific company, and it provides all the services required for the task. Many small growing enterprises can benefit from a private cloud, although it costs less to set up and requires minimal effort. Depending on the capital investment and corporate earnings, they may move to the next stage or even higher levels. The cost of setting up a private cloud varies. Cloud Stack, Rackspace, and Red Hat Cloud are some of the private cloud service providers.

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

2.1.2. Public Cloud:

The public cloud is for companies that want to share their resources, such as infrastructure, software, and platforms, with the general public. The Internet can be used to share resources and storage space. Public cloud services include Blue-Lock, Microsoft, and Google. Scalability, flexibility, cost-effectiveness, and geographic independence are all advantages of the public cloud. Google, HP, and Dell Inc. are among the public cloud suppliers.

2.1.3. Hybrid Cloud:

Both public and private clouds are used in a hybrid cloud strategy. Scaling across multiple clouds is a key feature of hybrid clouds. A hybrid cloud may require the use of both on-premises and off-premises resources. In hybrid clouds, fault tolerance can be met to a very high degree. For hybrid clouds to be a reality, workloads must be balanced across public and private clouds. Some of the hybrid cloud service providers are Voxon, VMware, and Western Digital.

2.1.4. Community Cloud:

According to the National Institute of Standards and Technology (NIST), the community cloud is described as a subclass of the public cloud in which diverse resources and services such as software, platforms, and infrastructure can be shared among multiple users [11]. In a crowded cloud market, the community cloud allows a variety of service providers to stand out. According to a Cisco survey, 90 percent of CIOs believe that the community cloud will be the most obvious on-demand approach. Intel Corporation and Cisco are two community cloud providers.

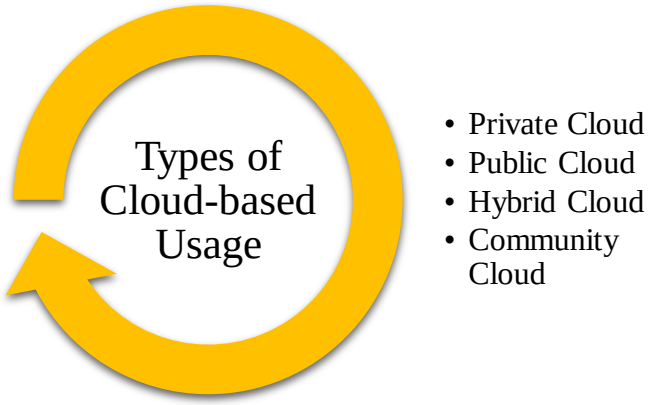

Figure 1: Demonstrating the Several Categories of Cloud-based Usages.

2.2. Data Security Lifecycle on Cloud:

Users may categories security problems using the fundamental CIA (Privacy, Integrity, and Availability) structure, which looks like the following in the cloud as shown in below Figure 2. Confidentiality attests to the adequate security of sensitive or confidential data stored or managed in the cloud. Depending on the requirements of the examined situation, it may be used to describe any or all of the following: the raw data kept outside, the traits of the people utilizing the data, or the actions that users carry out on the data. Integrity also depends on the reliability of the cloud's users, the accuracy of the data stored by outside suppliers, and the accuracy of the answers to

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

queries and calculations. To ensure availability, it is crucial to be able to establish and confirm that provider data complies with the standards outlined in existing service level agreements (SLAs) between clients and manufacturers. The particulars of the different scenarios will determine the challenges that must be overcome, the restrictions that must be removed, and the specific guarantees that must be provided to guarantee that the safety measures outlined above are satisfied. For instance, in a simple case when a worker just utilizes the data center for storage, concerns and problems include ensuring the security, confidentiality, and integrity of the data being stored as well as customer satisfaction regarding service level commitments.

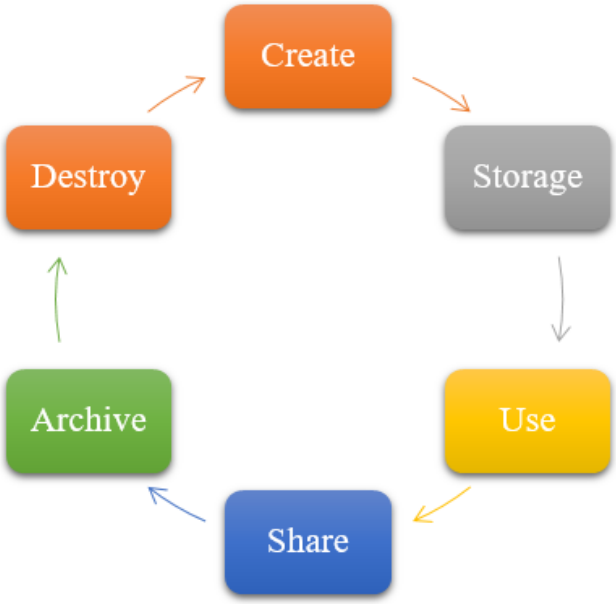

Figure 2: Indicating the Data Security Lifecycle on the Cloud.

3. CONCLUSION

Information security with regard to cloud computing is both challenged and given chances. Three sectors have undergone change: industrial development, safety regulation approach, and technological principles. As technology advances, users, service providers, and even government officials will need to consider their security requirements. Security is a problem for both users and cloud service providers. Those requirements could differ in some manner. Maintaining a balance between the needs of data protection and privacy protection is one of the most challenging problems we confront. This balance of requirements calls for a reevaluation of our technology paradigms. The creation of data security solutions must be encouraged to include infrastructure and service capabilities in addition to research and development. Users may get help from integrated service and infrastructure platforms in resolving a range of security issues. A shift in the approach taken by market regulators is reflected in the development of legislation and management. Authorities are worried about large-scale assaults in the cloud, unlike conventional licensing, which concentrates on safeguarding the essential communication networks. It is

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

important to note that the majority of the changes are improvements rather than radical departures from existing technological solutions.

REFERENCES:

[1] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing - The business perspective," *Decis. Support Syst.*, 2011, doi: 10.1016/j.dss.2010.12.006.

[2] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: State-of-the-art and research challenges," *J. Internet Serv. Appl.*, 2010, doi: 10.1007/s13174-010-0007-6.

[3] B. de Bruin and L. Floridi, "The Ethics of Cloud Computing," *Sci. Eng. Ethics*, 2017, doi: 10.1007/s11948-016-9759-0.

[4] I. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. Ullah Khan, "The rise of 'big data' on cloud computing: Review and open research issues," *Information Systems*. 2015. doi: 10.1016/j.is.2014.07.006.

[5] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *J. Internet Serv. Appl.*, 2013, doi: 10.1186/1869-0238-4-5.

[6] X. Xu, "From cloud computing to cloud manufacturing," *Robot. Comput. Integr. Manuf.*, 2012, doi: 10.1016/j.rcim.2011.07.002.

[7] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications*. 2017. doi: 10.1016/j.jnca.2016.11.027.

[8] P. Mell, "What's special about cloud security?," *IT Prof.*, 2012, doi: 10.1109/MITP.2012.84.

[9] P. Deshmukh, "Design of cloud security in the EHR for Indian healthcare services," *J. King Saud Univ. - Comput. Inf. Sci.*, 2017, doi: 10.1016/j.jksuci.2016.01.002.

[10] X. Chen, C. Chen, Y. Tao, and J. Hu, "A cloud security assessment system based on classifying and grading," *IEEE Cloud Comput.*, 2015, doi: 10.1109/MCC.2015.34.

[11] R. Kalaiprasath, R. Elankavi, and R. Udayakumar, "Cloud security and compliance - A semantic approach in end to end security," *Int. J. Mech. Eng. Technol.*, 2017.