Academic Guru Publication House

Advances in Cloud Computing Security
Techniques and Applications
Volume 1
Year: 2021

AG PH Books

A Review of Challenges and Security Risks of Cloud Computing

Dr. Algubelly Yashwanth Reddy[1*], Dr. P. Hasitha Reddy[2]

[1]*Head of the Department, Computer Science and Engineering, Sree Dattha Group of Institutions, Hyderabad*

[2]*Assistant Professor, Computer Science and Engineering, Sree Dattha Group of Institutions, Hyderabad*

Abstract

Because of its capacity to cut processing expenses, cloud computing is now one of the most hotly debated topics in the field today. The most intriguing and alluring technology of the present day is that which provides its customers with the ability to request services online. Because cloud computing stores as well as disseminates data in an environment, security has emerged as the primary impediment to the widespread use of the cloud computing settings. Many people utilise cloud to store our personal data, which necessitates a high level of the data storage security over media. When data is being uploaded to a cloud server, security is a key issue. The security dangers and problems of cloud computing are examined in just this review article, which also examines the security standards for cloud computing. Accordingly, the main purpose of this analysis is to categorise cloud computing security threats and issues.

Keywords: Cloud, security, solutions, challenges, risks.

1. INTRODUCTION

Computer services in the information technology such as platforms, infrastructure, or even applications may be set up and accessed through internet under the umbrella term "Cloud Computing. It is the large scaled distributed infrastructure in that shared resources are virtualized as well as services given to customers are dispersed in the terms of such virtual machines, deployment

[*] ISBN No. 978-81-955340-6-7

environments, or software. As a result, it's clear that cloud services may be dynamically scaled based on the current workloads as well as needs. According to the amount of resources that are consumed, the payment is paid based on that usage. One definition of 'cloud' is a'remote data centre,' as per [1]. There are two ways to look at it. First one is the use of a web browser to access information as well as data resources through the Internet. Secondly, the computer resources are paid for on a per-use basis. When you hear about "cloud computing," you're most likely thinking about the (NIST) National Institute of Standards and Technology since “a model for enabling universal, suitable, on-demand network access to share pool of configurable computing resources (e.g., servers, networks, applications, storage, and services) that can be rapidly released and provisioned with minimal management effort or service provider interaction” [2].

1.1. TYPES OF CLOUD

The range of the cloud computing architectures is vast, as well as the customer may pick which one best suits their needs and budget. It's basically as follows when it comes to cloud architecture [3].

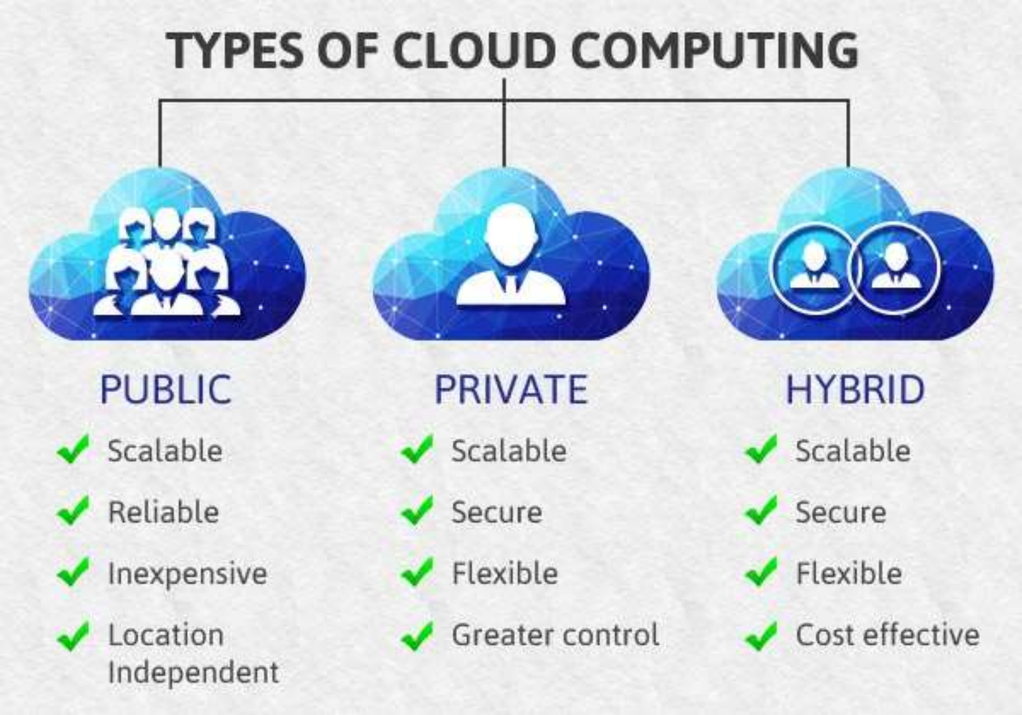

Figure1: Types of cloud [4]

- **Public Cloud:** Pay-as-you-go cloud computing is a sort of the cloud computing architecture that is designed for the customer in a pay-per-use paradigm. Google App Engine, or even Microsoft Azure and Amazon Web Services seem to be instances of this kind of service.
- **Private Cloud:** Designed for vital infrastructure as well as private businesses and organisations,

this sort of the cloud computing architecture. The cloud computing environment like this one is not open to the general public. A private cloud is indeed an instance of such a data centre owned by a private company or a government agency.

- **Community Cloud:** Third parties may use it to construct new apps as well as platforms for new services, and then it involves a wide range of diverse parties.
- **Hybrid Cloud:** There are public as well as private clouds in just this cloud computing structure. (NIST) that we called as National Institute for Standards and Technology defines it as “a hybrid cloud that has a combination of public and private clouds bound together by either standardized or proprietary technology that enables data and application portability” [2].

2. TYPES OF CLOUD SECURITY

- **Identity Security:** In terms of privacy as well as work, it is referred to as a technique. “ allows the authenticate people to retrieve the resources at the appropriatet time and for the good objectivess” [5]. It protects the privacy as well as security of data and applications while increasing their availability to authenticated individuals.
- **Information security:** Regardless of whether such data is encoded, transferred, processed, or the deposited, business practises must be in place to ensure that the data is protected at all times. [6].
- **Network Security:** The safety of a computer network is a precondition for its operation. Defending the current network infrastructure against unvarified individuals, violation, adjustment, breakdown, deterioration, or incorrect distribution is part of this process [7]. Because to issues at network level, web system's capacity as well as responsiveness might suffer, as well as overall latency.
- **Software Security:** It is necessary to start with the idea of the programme and work through the design and execution phases to build a security analysis procedure. In order to provide the highest degree of software security, each of these procedures is dependent on the others [8]. Even though complexity of such software development varies widely, everything requires a security assurance.
- **Infrastructure Security:** In order to verify the company's operations, it is essential that perhaps underlying infrastructure be secure. [9] Elements also need to be maintained apart. Users of the network may avoid having accessibility easily to the memory drivers or cryptographic codes by separating modules from the administration.

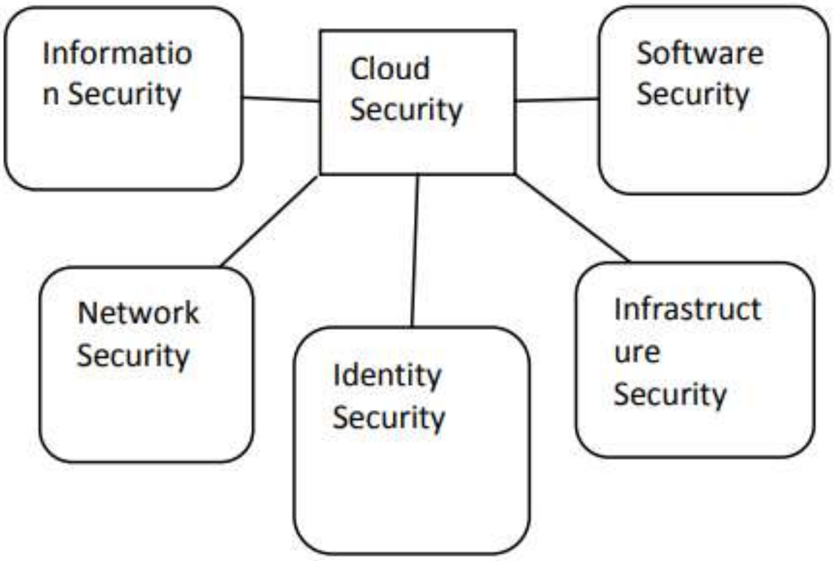

Figure 2: Types of Cloud Security.

Solutions: Cloud computing's security has been beefed up with the addition of a new encryption technique. The most common forms of encryption are attribute-based encryption, including homomorphic encryption, as well as symmetric encryption. Text security cypher or even key code are two options for attribute encryption. Encrypted messages and secret numbers billing encoded text that a customer leaves behind for the decryption are explained here. It is possible to decrypt encrypted material using the homomorphic encryption in CC. In order to safeguard sensitive data, it is necessary to use primitive cryptography in symmetric encryption. In order to provide high data protection, several types of encryption may be augmented with active solutions.

3. ATTACKS AND THREATS IN THE CLOUD SECURITY

The following is a list of cloud security assaults as well as threats:

- **Account and service hijacking:** Considered to be among the most dangerous dangers, Attackers target the web service hosted by the cloud service provider, as well as then install its control software inside cloud service provider infrastructure so that they may take control of such web service once it has been compromised. [12].
- **Backdoor Channel attacks:** This form of attack occurs in IaaS, whenever it delivers an effective customer's high penetration just on VM’s or even Hypervisor level. This may impair service availability as well as data privacy [13].
- **Cross site scripting attacks**: XSS is another name for it. It is among the most potent web

application security vulnerabilities that has been discovered to date. JavaScript is among the most often utilised programming languages in this kind of attack [12].

- **Cloud malware injection attack:** Injecting malware, the macules programme, or even a virtual machine into cloud infrastructure is among the most dangerous things you can do to your cloud computing security [14].
- **Denial of Service attacks:** When consumers try to use service after it has been compromised, it would not be accessible. They'll receive a 404 which is Not Found error [12] as a result. [12].

4. CLOUD COMPUTING CHALLENGES

- **Access controls:** Service providers should be concerned since it might expose user data as well as provide hackers access to an organization's infrastructure. [15].
- **Accounting:** In order to sustain network administration, it's an important factor to consider while installing cloud computing services [16].
- **Compliance:** The approaches of the compliance management are not well supported by cloud computing. Data security as well as privacy might be compromised as a result of this [16].
- **Cross-Organizational Security Management:** In the cloud computing, achieving and maintaining security as well as SLA compliance is a major difficulty. Cloud computing security can't be accomplished without the cooperation of several organisations [17].
- **Extensibility and Shared Responsibilities:** Cloud computing security is a topic that has to be addressed by both service providers as well as end users. Until recently, there has been no clear picture of how the cloud computing's security duties would be met. [18].
- **Private Cloud:** Due to the phrase "private cloud" meaning "on-premises," the working environment is supposed to be the same as in conventional computing. Through the use of virtualization technologies for computing resources, the computing resources are virtually extendable or de-extendable depending on the user's needs. This will give accessibility to shared resources for the entire departments in the organization. However, this has not been fully implemented in a wide range in the organizations. In other words, it is a halfway step to be implemented by the public cloud services [1].

Despite the fact that the concept of cloud computing has only just emerged. Cloud computing research is still in its infancy. Numerous concerns remain unresolved, as well as new difficulties continue to crop up across all industries on a daily basis. The follows are some cloud computing research issues to keep an eye on.

- Service level agreement (SLA)
- Cloud data management and security
- Data Encryption
- Virtual machines migration

- Access controls
- Multi-tenancy
- Reliability and availability of services.

5. FUTURE ADVANCES IN THE FIELD OF CLOUD COMPUTING

A concept termed as Automation is taking hold in IT business during the next five years. AI as well as ML are likely to play an important part inside automation process within next five years, at least. Programming-related professions in the IT sector are likely to become less common as automation advances. To illustrate the point, let's take a look at a hypothetical situation. When a computer replaces human brain in logic-building process, we can envisage the harm that will be done in terms of the INTRUSION. It takes a reasonable length of the time for a typical programmer to conduct (or) complete the specified task. Considering today's technology as well as the knowledge it gained via machine learning, a machine can do the identical task in a matter of seconds. Traditional IDS systems might be ineffective in this case because of the increased automation. As a result, there is a pressing need to bolster existing security measures, such as fire walls as well as IDS.

6. CONCLUSION AND FUTURE WORK

Using cloud computing is enticing because of its adaptability, effectiveness, usefulness, as well as cost-savings features. It's the newest and most promising technology, but it's also vulnerable to a variety of threats. Data security challenges and methods for dealing with them are discussed here in order to deal with the CC risks.

Recently, both the business and academic worlds have taken a keen interest in the cloud computing, which many see as a foundation for the contemporary societies of future. Economic improvements as well as cost savings may be achieved by using cloud computing. Empowering cloud computing qualities are sought by governments, organisations as well as enterprises. There are still many security as well as privacy concerns that must be addressed before cloud computing can be widely used in the next several years. The most recent threats and difficulties associated with cloud computing have indeed been explored in this study. Developing a security model that takes into account the dangers and difficulties that have been highlighted will be the focus of our next research.

References

1. Kim, W., et al. Adoption issues for cloud computing. in Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia. (2009). ACM.

2. Mell, P. and T. Grance, Draft nist working definition of cloud computing. (2009)
3. Subbiah, M., D.S.S. Muthukumaran, And D. Ramkumar, Enhanced Survey And Proposal To Secure The Data In Cloud Computing Environment. International Journal Of Engineering Science, (2013) .
4. Ali, Alwesabi, Almutewekel Abdullah, and Okba Kazar. "Implementation of cloud computing approach based On mobile agents." International Journal of Computer and Information Technology 2.06 (2013): 2279-0764.
5. S. Hajra et al., “DRECON: DPA Resistant Encryption by Construction,” Springer, 2014, pp. 420–439.
6. A. Tripathi and A. Mishra, “Cloud computing security considerations,” IEEE Intl.Conference on 90Signal Processing, Communications and Computing (ICSPCC), 2011, pp. 1–5
7. “SANS Institute: Network Security Resources.” [Online]. Available: 91https://www.sans.org/network-security/. [Accessed: 16 Feb. 2017]
8. M. Al Morsy, J. Grundy, and I. Müller, “An Analysis of the Cloud Computing Security Problem,”APSEC Cloud W., Nov.2010.
9. K. M. Khan and Q. Malluhi, “Establishing Trust in Cloud Computing,” IT Prof., vol. 12 (5), Sept. 2010, pp. 20–27.
10. N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. Ràfols, “Attribute-based encryption schemes with constant-size ciphertexts,” Theor. Comput. Sci., vol. 422, Mar.2012, pp. 15–38.
11. Younis, M. and K. Kifayat, Secure cloud computing for critical infrastructure: A survey. Liverpool John Moores University, United Kingdom, Tech. Rep, (2013).
12. Modi, C., et al., A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications, 36(1) (2013). 42-57.
13. SUBBIAH, M., D.S.S. MUTHUKUMARAN, and D. RAMKUMAR, Enhanced Survey and Proposal to secure the data in Cloud Computing Environment. International Journal of Engineering Science, (2013) 5.
14. Chou, T.-S., Security threats on cloud computing vulnerabilities. International Journal of Computer Science & Information Technology, 5(3) (2013) 79.
15. Zissis, D. and D. Lekkas, Addressing cloud computing security issues. Future Generation computer systems, 28(3) (2012) 583-592.
16. Moreno-Vozmediano, R., R.S. Montero, and I.M. Llorente, Key challenges in cloud computing: Enabling the future internet of services. Internet Computing, IEEE, 17(4) (2013) 18-25.
17. Khalil, I.M., A. Khreishah, and M. Azeem, Cloud computing security: a survey. Computers, 3(1) (2014) 1-35.
18. Zhang, L., et al., Cloud manufacturing: a new manufacturing paradigm. Enterprise Information Systems, 8(2) (2014) 167-187.