An extensive study of different cloud services and its security concerns and challenges

[1]Yaswanth Arikatla, [2]Veera Brahmam Ainala, [3]Varma Seru, [4]Sahil Dasu, [5]Dr. B. Bikram Kumar

Dept. Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation,
Vaddeswaram, Guntur, India.

***Abstract*- Cloud computing has become one of the world's most important emerging technologies. It helps the users to store abundant data which helps the users to get access to that data by using the internet. It allows users to use multiple applications and programs in one or more systems at the same time. It has features that attract everyone from enterprise companies to personal users. Along with the massive increment in the usage of the cloud, security issues[6] are also increased. Data security is a major threat to cloud users as all the services and features are accessed through the internet. Here in this paper, we explained different service models in the cloud, and their features and exposed the major security threats and their countermeasures to protect the data in the cloud.**

***Index Terms*- Cloud Computing, Cloud Service Models, Cloud Deployment Models, Cloud Security, Cloud Attacks and Cloud Security Solutions.**

I. INTRODUCTION

Cloud computing helps to provide the computing services with the help of internet all over the world, which includes processors, memory, data, networks, technology, statistics, and information (Internet)[1]. The cloud can be used in place of an on-site datacenter. We have to control everything within the on-premises datacenters which includes the purchasing and installing of hardware and virtualization, installing the operating systems and required software's, configuring the network, configuring the firewall, and configuring data storage. After completing all of the setup, we now in charge of maintaining it for the rest of its life. The term "cloud computing" refers to the remote control, configuration, and access to hardware and software resources[1][6]. Infrastructure, applications, and online data storage are all made available. Cloud computing provides platform independence because the software does not need to be physically installed on the PC.

Modern corporate apps are now mobile and collaborative due to cloud computing[7]. Many aspects of daily life have been affected by the wide range usage of cloud based software and making it difficult to calculate the usage effect of cloud computing on businesses and end users. By leveraging cloud computing, startups and businesses can save money and expand their offerings without having to buy and maintain their own equipment and software[7]. Independent developers have the authority to release internet services and benefits to the general public. Data sharing and analysis are now possible at scales previously reserved for well-funded projects. Furthermore, internet users can easily access programs and storage to create, distribute, and save digital media in quantities far exceeding the capabilities of their personal computers. Many of the same security controls, technologies, practices, and procedures used to protect physical data centers, networks, and compute environments are included in cloud security (also known as cloud computing security)[8][15], with the exception that they are implemented as a service to protect your cloud data. Securing cloud assets is one of the shared responsibility model among cloud providers and the clients.

Many Cloud service providers such as Amazon Web Services (AWS), Google Cloud, and Microsoft Azure, uses Shared Responsibility Model to show who is responsible for their sensitive data and its storage path. According to Amazon, "cloud security" refers to the infrastructure that enables cloud services, whereas "cloud security" refers to the deployments, virtual servers, and apps that are used.

Numerous people believe that cloud security is more difficult to implement than traditional data security[4][8] because cloud operations remove some of the customer's access and control. That is partially correct, but cloud security may be more manageable than on-premises security in several ways. A portion of the burden for securing operations falls on the cloud provider, and cloud security systems also allow users to manage cloud assets from a dashboard or centralized location. Furthermore, the cloud relieves the customer of some of the burden of network and physical security. To summarize, cloud security does not have to be extremely difficult if properly implemented.

II. Literature Review

We examined many websites in order to comprehend the fundamentals of cloud computing and how to maintain data security[9] within each cloud. The literature study in this part provides a foundation from which to discuss various aspects of cloud security. Yaswanth and Veera Brahmam gave some excellent information on the fundamental ideas of cloud computing. This article examines the principles of cloud computing and can help the developing world make use of cutting-edge technologies [1].On the other side, Yaswanth and Varma have discussed the security concerns that cloud users have[2].Security issues[5][13], according to Varma and Sahil, are one of the major obstacles preventing large enterprises from relocating their data over to the cloud.

III. Architecture Of Cloud

As every cloud provider provides the users both platform and underlying IT infrastructure, clouds are regarded as Platforms-as-a-Service (PaaS). To establish and supply consumers with the cloud infrastructure, providers must do more than simply abstracting the capabilities of computer from its hardware[1][3]. Software integration for containerizing, orchestration, API's, routing, security management, and automation are also necessitates for extra development tiers. To build an accessible online experience, user experience design (UX) is crucial.

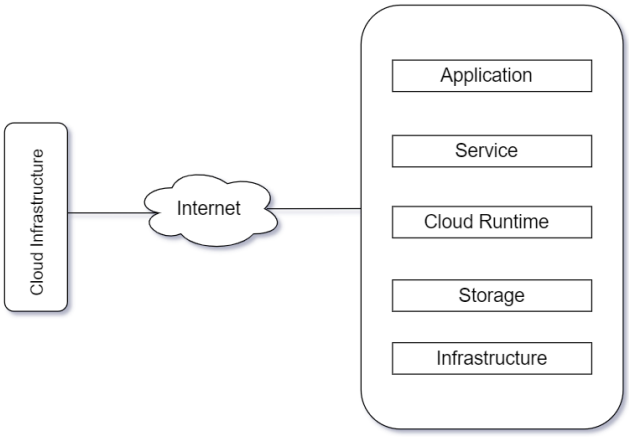


Figure 1 Simple architecture of Cloud

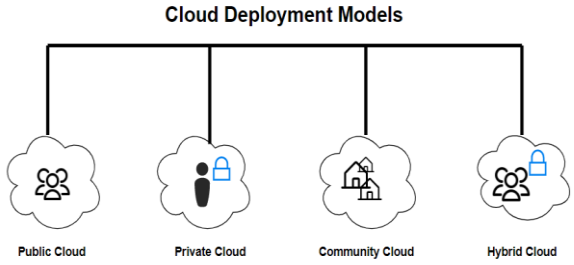
A. Cloud Deployment Models

An individual cloud environment is denoted by a cloud deployment paradigm based on who is in charge, who has access, and whether resources are shared or allocated.

It outlines your cloud infrastructure's appearance, your level of customization, and whether you will receive services. The relationships between your users and the infrastructure are also represented by the various cloud deployment types.

Types of different Deployment Models: -

1. Public Cloud
2. Private Cloud
3. Community Cloud
4. Hybrid Cloud



Public Cloud:-

Everyone can be able to use public cloud for accessing systems and cloud services and it is open to all but in security segment it is less secured. In public cloud infrastructure services are available all over the internet for public or any industry groups. The infrastructure in public cloud model is owned by the organisation that provides the cloud services, not the user.

Users can now access the systems and several cloud services easily, thanks to this type of cloud hosting. Public cloud is a perfect example for cloud hosting, where service providers provide their services to diverse set of clients/users. This type of arrangement provides storage backup and retrieval services for free or a subscription basis, or per user.

For example: Consider Google App Engine.

Private Cloud: -

Public and private clouds' deployment models[11] differ significantly from one another. There is only one user, thus it is a private area. It is not necessary to let others use your hardware. How you manage all the hardware differs between private clouds and public clouds. The term "internal cloud," which also refers to the capability of accessing systems and services that are hosted inside a certain business or border, is another name for it.
The cloud-hosted, fortified by powerful firewalls, and managed by an organization's IT department, the cloud platform is used in a highly secure environment. More independence and control over cloud resources are available with the private cloud.
Community Cloud: -

It makes systems and services accessible to many enterprises. In order to serve the needs of a community, industry, or company, a distributed system was developed by combining the services offered by many clouds. The group that shares common goals or responsibilities may share the group's infrastructure. Usually, a third company or a group of local organisations are in charge of managing it.
Hybrid Cloud: -

Hybrid cloud computing combines the best aspects of both worlds by using a layer of open source software. You can host the app in a secure place and gain from the financial advantages provided by the public cloud by utilising a hybrid solution. Depending on their needs, organisations may mix two or more cloud deployment approaches to move data and applications between different clouds.

B. Cloud Service Models

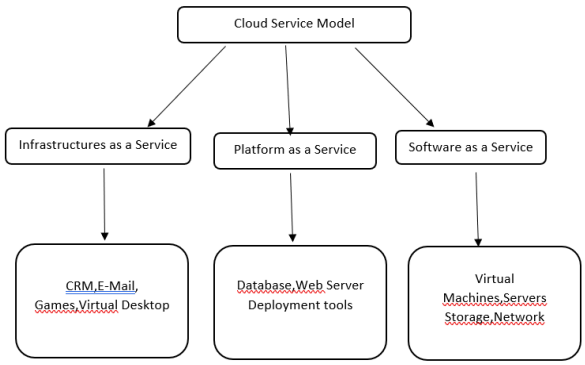


Figure 2 Cloud Service Model

- Infrastructure as a Service:

It provides the business companies to use IT services which are used to develop environments, networks, secured data storages and tools for any software development and the application testing. The industries don't need to newly develop and secure their infrastructures the cloud service provide the full tools and services which are needed to develop any infrastructure and cloud storage backups. AWS, GCP and Azure are the most used services by many enterprises.

- Software as a Service:

It plays a vital role as a platform to provide the services of any web applications to its end users to access the cloud computing services through internet. It can be easily accessed through the web browser. It provides the continuous delivery to the customer. It is fully managed by the cloud providers from deployment to hosting. It helps with huge data storages for the companies who use the cloud services. We can also modify and develop environments using SaaS where developers can modify and develop a product.

- Platform as a Service:

It is an environment for any cloud/software applications, where it can also be used as a platform to build applications as like IaaS. It provides the environment tools to its users and acts as a platform for any software applications. In this, the users don't have any access to the infrastructure services which are OS and application tools . However, they have control over the apps that will be created and deployed.

IV. CLOUD SECURITY

Another type of cyber security that helps in protecting cloud computing is cloud security[4]. It defends against a variety of cloud security issues[5][6], such as data security, governance, access control, compliance, and data misconfiguration[2][9]. It is a collection of several protocols, technologies, and practices that helps in securing cloud environments, applications, and data that is stored there.
Cloud Security includes a variety of techniques to maintain data security in cloud computing, including safeguarding networks and data storages against intentional data thefts, retrieving lost data, and identifying and fixing human errors that result in data leaks and system compromise.

- How service models impact on cloud security[11]

Based on the Cloud Services and Cloud Environment we can achieve the target of securing cloud components[2]. There are various cloud services that are used to create cloud environments for individuals. Users can access software programs using a web browser thanks to the software as a service (SaaS) delivery model. Similar to IaaS, Platform as a Service (PaaS) is a cloud-based software environment that may also be used as a platform for developing applications. We can virtualize out-of-date resources thanks to a service called Infrastructure as a Service (IaaS) and access them over the internet. These are the main services that contribute to the provision of cloud services.

A. Cloud Attacks

- Cloud Malware Injection: Which helps the attackers to control the user's data in cloud[9], for this they add a malware infected service to SaaS/PaaS/IaaS services.
- Denial of Service Attacks: These DDoS attacks are mainly designed to overload a system by sending the infinite requests to the systems and make the services to stop and not available for its users.
- Side Channel Attack: In this the hackers place a infected virtual machine to the target and during this they targets the system configuration algorithms and it can be avoidable by securing the system algorithm.
- Wrapping Attacks: It is an example of man in the middle attacks in cloud computing. It allows the attackers to manipulate the XML document which is used to protect the user's credentials from unauthorized attacks.
- Insider Attack: It is mainly done by the insiders of an organization who are employers or cloud service providers by violating the company policies. It can control by giving the different levels of access permissions to cloud services.

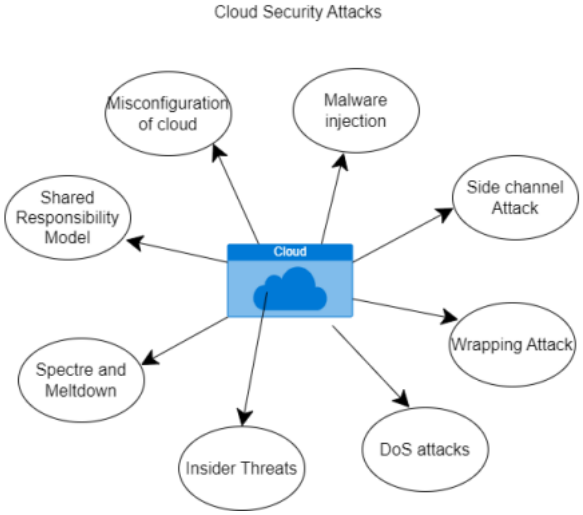


Figure 3 Cloud Security Attacks

V. CLOUD SECURITY SOLUTIONS

- **Cloud Access Security Brokers:**

Between cloud service consumers and cloud service providers, this are on-premises or cloud-based security policy that integrate and inject enterprise security policies[5] such as accessing the cloud based services[2][4]. The execution of numerous security policy types is consolidated by CASBs. The following security procedures are covered by security policies such as authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention, and other security rules[5].

- **Cloud Security Posture Management:**

CSPM discovers and displays cloud security configurations and infrastructure assets. Users can access a single source of truth across multiple cloud environments and accounts. Cloud resources and details, such as configuration errors, metadata, networking, security, and modification activity, are discovered immediately after deployment. Accounts, regions, projects, and virtual networks are all administered through a single console.

- **Static Application Security Testing:**

SAST searches for code patterns that signify widespread vulnerabilities by looking at an application's source, binary, or byte code. This is done by modelling the application, the code, and the data flows. This architecture enables the SAST solution to apply specified rules to find known categories of vulnerabilities.

- **Secure Access Service Edge:**

No matter where their users, workloads, devices, or applications are located, an organization can ask for secure access using a SASE strategy when it is appropriately configured. This turns into a crucial benefit for ensuring the security of distant personnel. Applications as a service (SaaS) are widely used, and data is transferred quickly across data centres, branch offices, and hybrid and multi-cloud systems. Safe browsing, secure access to business software, and secure access to SaaS applications are all made possible by SASE.

VI. CONCLUSION

Cloud computing has grown dramatically in the last ten years, with significant breakthroughs and advances being widely used in a variety of industries due to a more useful service and ease[5]. Enterprises and organizations benefit from implementing cloud technologies within their organizations. However, the widespread use of cloud computing, combined with the fact that the service is dependent on an internet connection, makes it vulnerable to a variety of security threats, making cloud security a critical component of computer security. This study thoroughly examines the major threats to cloud security[12]. Countermeasures and threat mitigation techniques are also provided as advice. Similarly, comprehending cloud security challenges[6] and practical solutions[10][15] is critical to mitigating the risks associated with cloud computing adoption.

REFERENCES:

1. Voorsluys, W., Broberg, J., and Buyya, R. (2011). Introduction to Cloud Computing. In R.Buyya, J. Broberg, A.Goscinski. Cloud Computing: Principles and Paradigms. New York, USA: Wiley Press.
2. Krutz, R. L., & Vines, R. D.(2010). Cloud Security: A comprehensive guide to secure cloud computing. Wiley Publishing.
3. Antonopoulos, N., & Gillam, L.(2010). Cloud Computing Principles, Systems and Applications
4. Ahmed, H. (2014, July). Cloud Computing Security threats and Countermeasures. Retrived October 2, 2018, from https://pdfs.sematicscholar.org/8ee8/7566633a384d3289ffdee687b3df08940b27.pdf
5. Johnson, R. (2015). Security policies and implementation issues (2nd Ed.). MA: Jones & Barlett Learning.
6. Kashyap, R. % Sharma, S.(2015). Security challenges and issues in cloud computing - the way ahead. International Journal of Innovative Research in Advanced Engineering, 9(2), 32-35.
7. Armbrust, Michael, Fox, Armando, Friffith, Rean, et al. "Above the clouds: A Berkely View of Cloud Computing" Feb 10, 2009.
8. Ramchandra, G., & Iftikhar, M. (2017). A Comprehensive Survey on Security in Cloud Computing. Elesvier, 465–472.
9. B. Priyadarshini and P. Parvathi (2012), “Data Integrity in Cloud Storage ,” IEEE, no. 978-81-909042, pp. 261–265.
10. Rao et. al, - Data Security Challenges and Its Solutions in Cloud Computing, ICCC 2015, Procedia Computer Science 48 (2015), Pages 204-209.
11. K.Jamsa, Cloud Computing: SaaS, PaaS, IaaS, Virtualization, Business Models, Mobile, Security and More. Burlington, MA, USA: Jones & Bartlett, 2012.
12. I. A. T. Hashem et al., “The rise of “big data” on cloud computing: Review and open research issues,” Inf. Syst., vol. 47, pp. 98–115, Jan. 2015.
13. G. S. Varsha Wadhwa A, " Study of Security Issues in Cloud Computing," International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 4, Issue. 6, pp. pg.230-234., June 2015 .
14. M. I. F. K. G Ramachandra, "A Comprehensive Survey on Security in Cloud Computing," in Procedia Computer Science, 2012 , 2017.
15. D. B. M. Pradeep Kumar Tiwari1, "Cloud Computing Security Issues, Challenges and Solution," ijetae, ISSN 2250-2459, Volume 2, Issue 8, August 2012.