Journal of Innovative Engineering and Research (JIER)
Vol.- 3,Issue - 2,October 2020, pp. 12-15 (4 pages)

A Basic Study on Cloud Security Challenges

JAYA SHARMA, Dr. SANJAY SINGH BHADORIYA

Department of Computer Application, Dr. A. P. J. Abdul Kalam University, Indore
Corresponding Author Email: jayasharma.cs@gmail.com

***Abstract*— Cloud computing is the most emerging technology nowadays due to its various computing infrastructure and services. It comes with various features and services which makes new possibilities for different business organizations and IT industries. Cloud computing provides a large number of services as per the need of a user. It includes infrastructure, platforms, storage, data servers, networking, and software.**

Cloud computing infrastructure and services come with security challenges too. This paper describes cloud computing, its services models, security threats, basic information about solving security threats through machine learning, and some of the key research topics in this area are discussed.

***Index Terms*— Cloud computing, services models, security threats, Machine learning.**

I. INTRODUCTION

Cloud computing is an application-based software infrastructure thatstores data and accessing program through the Internet to provide a large number of services like including servers, networking, storage, software, databases, analytics, and intelligence—over the Internet to offer faster innovation, economies of scale and flexible resources. Cloud computing allows users and organizations to use applications without installation and access their data files at any computer with internet access. Cloud computing is offered in three different service models are known as software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS). Cloud service provides an important feature of cloud computing is on-demand services mean end users can request according to need. SaaS, PaaS, and IaaS provide services such as platform and infrastructure, software, storage, networking, according to user needs. it is important to provide security in cloud services

Major threats to cloud security include, data loss, data breaches, insecure application program interfaces (APIs), service traffic hijacking, account hijacking, weak control plane, shared technology that can compromise cloud security, and poor choice of cloud storage providers.

Cloud security is an important key concern for cloud Service providers. They must follow certain regulatory requirements for storing sensitive data such as health information, credit debit card numbers, bank account detail, social contacts and satisfy their customers. Third-party audits of a cloud service provider's security systems and procedures help ensure that users' data is secure and safe.

Machine learning approach for enhancing the accuracy of automatic spam detecting, filtering, and separating them from legitimate messages. In this regard, for reducing the error rate and increasing the efficiency.

II. CLOUD COMPUTING SERVICES MODELS

There are three different types of cloud computing services models

Software-as-a-Service (SaaS): Software-as-a-service refers to the use of various web-based applications that run and execute on the server. The SaaS model provides only hosted applications. By using this model, we can reduce the cost of hardware and software development, maintenance, and operations.

Platform-as-a-Service: Platform-as-a-Service model involves the use of the operating system and development tools in the cloud. In this model, the customer can develop his application on the provider-supported platform. By using this model we can reduce the cost and full management complexity. The customer can manage his required software components of the platform. The development environment is determined by the cloud provider. The cloud customer has control over the applications and application environment settings of the platform.

Infrastructure-as-a-Service: It is the hardware component with different forms of virtual technology rentals. In this model, the provider hosts the consumer's virtual machines and thereby provides networks and storage. By using this module the customer avoids purchasing and managing the hardware and software infrastructure components and is provided with all resources virtualized through a service interface. [1]

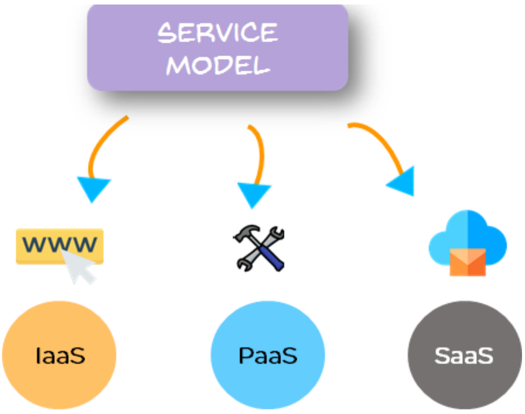

Figure 1: Cloud service model

III. CLOUD DEPLOYMENT MODEL

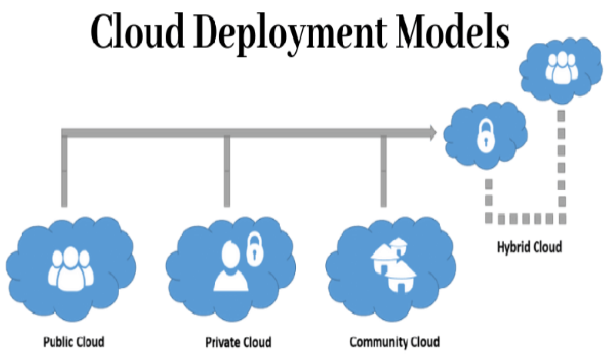

Figure 2: Cloud Deployment Model

The National Institute of Standards and Technology (NIST) submitted a review in January 2011 According to NIST,

The four main models for implementing cloud computing are:

Public cloud: As the name itself indicates, the infrastructure is open for public use. In this model, the provided cloud infrastructure can be used by many customers and is organized by a third party [2].

Private cloud: The cloud infrastructure can only be used for specific clients and is organized by the company itself or a third-party service provider. It is carried by the concept of a virtual machine and is a private network.

Community Cloud: As the name suggests, this is an infrastructure shared by several companies to achieve a common goal and can be organized by them or by third-party providers [3].

Hybrid cloud: This combination of two or more cloud distribution methods has clear differences and does not interfere with each other [4].

In the overview, the cloud platform must have the following properties:

On-demand service - "pay as needed"
Accessibility via browser
Resource sharing
Fast flexibility
Services for consumers

The service provided to consumers is Infrastructure as a Service (IaaS) - as Amazon Elastic Compute Cloud (Amazon EC2) [5], Platform as a Service (PaaS) example Microsoft Azure [6] and software as a service (SaaS) -like YouTube, Facebook. The growing popularity of cloud computing has led most companies to try to adapt to the cloud. The benefits of reducing the cloud computing area include initial infrastructure costs, availability, flexibility, and pay-per-view. Usage, on-demand services, and easy maintenance and updating. In addition to security issues, some of the disadvantages of using the cloud are lack of control, data recovery, service level agreements, legal issues, and evaluating and evaluating the performance of the cloud environment are major frustrations [7]

IV. CLOUDS SECURITY

When customers want to transfer their data and their applications, security has always been an issue. Security plays a key role in protecting cloud services. We need to prove the importance and motivation of security in the transmission of older systems, and when we move our business to the cloud to discover conditions, concerns, conditions, aspects, benefits, and advantages of security, we need to consider dealing with security Different methods. Providing security in a private cloud is cheaper than a public cloud, but it is more difficult for a hybrid cloud because it is not the only hybrid, private or public cloud with a provider Cloud services. It is more difficult to establish hybrid cloud security with multiple service providers, especially for large-scale distributions and optimizations.

Cloud computing will pose security threats, some of which are as follows:

Network Security Threats - Network Security is defined as a method of protecting network security, and any attempt to violate the confidentiality, integrity, and availability (CIA) of security is defined as an intrusion. In network security, cloud computing security is an important subdomain. Cloud security consists of a set of policies, applications, methods, and cloud security infrastructure [8].A network security threat is trying to get illegal access to your organization's network, hack your data without your knowledge, or execute other malicious acts. The network security is at risk or vulnerable if there is a vulnerability or weakness within your computer network.

Data Security (Data Loss/Leakage)Threats - In data Security threats can be many like theft of intellectual property Software attacks, theft of equipment or information, identity theft, and information extortion.

Application Security Threats - There are various application threats that users and app developers should understand and manage. Some of the common ones include malware, brute force, and injection attacks for example Brute force attack are techniques used by hackers to hack by using common passwords used among people.

Web Security Threats -web threats refer to malware software programs that can target your computer when you're using the internet. These browser-based program threats include a range of malicious software programs that are designed to affect target computers.

Encryption and Key Management Security Threats – Sometimes organizations failed to properly use encryption algorithms and use insecure cryptographic implementations and fail to store encryption keys securely. They may not have a robust authorization, which usually opens data to be accessible and may lead to data loss if encryption keys are lost.

Server Security Threats –a large amount of organization's information, user information hold by the Server. Server security is also important same as network security. If server security is compromised, it may open the organizational data for hackers to steal or manipulate.

Virtualization Security Threats- The concept of virtualization helps to divide a physical computer into several logical computers and then isolate them in whole or in part. These logical partitions are usually called virtual machines (VMs) or guest machines [9].Virtualization design, implementation, and deployment have also opened the security threats and security issues.

Authentication& Authorization Security Threats – Authentication specifies how a system finds who you are, and authorization specifies how much access you have to read, write and edit the information in the system. System authentication and authorization are attacked for gaining access to the system resources without the correct authorization.

Malicious Insiders - Malicious insider an insider threat. This threat is a security risk that originates from within the targeted organization. A malicious insider knew as a Turncloak, if someone inside of an organization who has access to organizational information intentionally gains and uses someone else's credentials, usually to get information of financial or personal data.

Other security challenges are denial of service (DoS distribution, HDoS, XDoS, anti-IP staff, backing up your IP vulnerabilities, dictionary attacks) as well as their intentions of losing and remedying many cloud network users. These groups perform and read interlayer attacks means to reverse back to the network to stimulate communication and send messages Convert to expected attack. They are following;

Denial of Service (DoS) Attack: separate flooded by a large number of needs.

Distributed DoS Attack (DDoS): make a longer version of the DoS attack and flood it with several packets. The traditional DISTo (Distributed Denial of Service) attack has evolved into a new type of threat, called the "Economic Denial of Service (ESS)" attack [10]. Attackers are focusing on consuming more and more cloud resources by consuming operating budgets without creating any business for hosting services to cause financial losses.

HDoS (HTTP Post DoS) Attack: Slows down transmission of messages or packets in the network.

PDoS (Permanent Denial of Service) Attack: It is a hardware targeted attack. It is very fast and requires fewer resources to damage the system badly.

XDoS (XML DoS) Attack: This is an unusual attack. This happens when an error in the trusted client program enters an unlimited number of connections. The purpose of the attack is to shut down web services or service systems.

Man-in-the-Middle Attack- The attacker can place himself in the communication path and can stop and change the communication at any time.

Rejection - In the process, they attempt to reject the submitted content or deny the validity of the submitted statement or agreement.

Elevation of Privileges- Attackers can gain unauthorized access to information and resources.

Virus and worm attacks are common and well-known attacks, and these code segments are malicious code for operating hardware and software, though malicious code can corrupt files in the local file system.

Spoofing attack: When a malicious hacker attacks a network computer user or computer, the program launches and steals the network host, spreads viruses, or monitors it.

V. FEATURES FOR CLOUD SECURITY CHALLENGES

The benefits of the cloud are plagued by security concerns. Security has become more challenging in the cloud and or the virtualization environment due to multiple entry points and interconnection points in VM. A Cloud system is said to be secure if it has at least these five important features [11] -availability, confidentiality, integrity, control, and audit. Although it is desired, it is not easy to achieve all the five features together.

Availability

Availability is attributed to cloud resources that are available anytime, anywhere [Twenty-four]. Ease of use can be improved by enabling comprehensive Internet access, although users will still rely on the timely provision of resources. Accessibility is a major issue in cloud computing because more accessibility shows higher reliability. In the past, the most trusted CSPs like Amazon, Google, and Microsoft experienced unexpected downtime [12]

Confidentiality

Confidentiality is attributed to the ability to keep user data secure and confidential in the Cloud system. To attract more users to use the cloud, CSPs need to be more confident in confidentiality requirements [13].

Completeness

Data integrity in the cloud environment is attributed to the protection of information integrity, i.e. Data protection against being lost or altered by unauthorized users [14].

Control

Cloud Control is attributed to the usage regulation of the cloud system, including the applications, infrastructure, and data. Cloud computing technology benefits organizations in a way to accomplish more by paying less in the long run. Giving up direct control of the data has been the hardest thing for organizations. Control over data, functionality, assets, and access are the main control types that organizations are worried about [15].

Audit

Cloud Audit attributes to watching and monitoring what has occurred in the Cloud environment. Auditing facilitates the ability to watch what is happening in the cloud environment and acts as an additional abstract layer on top of the virtual application environment. The three crucial activities of the audit are Events, Logging, and Monitoring. These days with the help of cryptography, verification of remote data is performed by third-party auditors (TPA) [16].

VI. RECOMMENDED SECURITY MEASURES

Many algorithms have been created for the above security challenge but machine learning is still used a lot to protect cloud computing. The machine learning algorithm automatically learns the entire input data and extracts functions for classification. In addition, machine learning algorithms have a large number of hidden layers to learn and obtain the overall properties of data, hidden information, and other additional meta-information. It helps to make an accurate classification. The machine-learning algorithm allows software applications to produce accurate predicting outcomes without being explicitly programmed. The machine learning algorithm can be divided into classification algorithms and clustering algorithms. [17].

VII. CONCLUSION

Cloud Computing is an approach that gives several benefits and it also comes with some security issues which may affect its users. In this paper, we have discussed the basic concepts of cloud computing, its services, different security threats and security features. We have also discussed possible solutions for security threats through the basic concept of machine learning. There are many areas of research on the migration of hereditary systems. Sooner or later, the company hopes to rewrite or replace old or embedded applications in modern architectures, migrate to the cloud, and manage remotely. To this end, we need to consider the security of this process and develop a migration process to adjust and transform security features to request legacy inheritance to cloud-based security services.

REFERENCES

1. Shazli Hasan Khan “Cloud Computing Transforming The Dynamics Of Teaching Learning Process In Higher Educational Institutions Of India “International Journal of Recent Scientific Research Vol. 10, Issue, 07(E), pp. 33645-33652, July, 2019.
2. Mazzariello C, Bifulco R, Canonico R. Integrating a network ids into an open source cloud computing environment. In: 2010 sixth international conference on information assurance and security, pp. 265–270, IEEE; 2010.
3. Modi C N, Patel D R, Patel A, Rajarajan M. Integrating signature apriori based network intrusion detection system (NIDS) in cloud computing. Procedia Technol 6, 905–912, 2012.
4. Dou W, Chen Q, Chen J. A confidence-based filtering method for DDos attack defense in cloud environment. Future Gener. Comput. Syst. 29, 7, 1838–50, 2013.
5. Negi P., Mishra A., Gupta B. B.. Enhanced CBF packet filtering method to detect DDos attack in cloud computing environment. 2013. ArXiv preprint arXiv:1304. 7073.
6. Ismail M N, Aborujilah A, Musa S, Shahzad A. Detecting flooding based dos attack in cloud computing environment using the covariance matrix approach. In: Proceedings of the 7th international conference on ubiquitous information management and communication , pp. 1–6, 2013.
7. Vissers T, Somasundaram T S, Pieters L, Govindarajan K, Hellinckx P. DDOsdefense system for web services in a cloud environment. Future Gener. Comput. Syst. 37, 37–45, 2014.
8. Lau F, Rubin SH, Smith M H, Trajkovic L. Distributed denial of service attacks. insmc 2000 conference proceedings. 2000 ieee international conference on systems, man and cybernetics. ’cybernetics evolving to systems, humans, organizations, and their complex interactions, Vol. 3, pp. 2275–2280, 2000.
9. Tan Z, Jamdagni A, He X, Nanda P, Liu R P. A system for denial-of-service attack detection based on multivariate correlation analysis. IEEE Trans Parallel DistribSyst 25, 2, 447–56, 2013.
10. Somani G, Gaur M S, Sanghi D, Conti M. DDoS attacks in cloud computing: collateral damage to non-targets. Comput. Netw. 109, 157–71, 2016.
11. Aborujilah A, Musa S. Cloud-based DDos HTTP attack detection using covariance matrix approach. J Comput. Netw. Commun. 2017.
12. Behal S, Kumar K. Detection of DDos attacks and flash events using novel information theory metrics. ComputNetw 116, 96–110, 2017.
13. Singh K J, De T. MLP-GA Based algorithm to detect application layer DDos attack. J. Inf. Secur. Appl. 36, 145–53, 2017.
14. Sahi A, Lai D, Li Y, Diykh M. An efficient DDos TCP flood attack detection and prevention system in a cloud environment. IEEE Access, 5, 6036–48, 2017.
15. Chen MH, Chang PC, Wu JL. A population-based incremental learning approach with artificial immune system for network intrusion detection. Eng. Appl. Artif. Intell. 51, 171–81, 2016.
16. Zhou B, Li J, Wu J, Guo S, Gu Y, Li Z. Machine-learning-based online distributed denial-of-service attack detection using spark streaming. In: 2018 IEEE International Conference on Communications , pp. 1–6, 2018.
17. Dhivya, Dharshana, Divya “Security Attacks Detection in Cloud using Machine Learning Algorithms”, IRJET, Volume: 06 Issue: 02, Page 224 – 230, Feb 2019.