IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Security on Cloud Infrastructure - A Review

[1] Mr. Aniket Ghate

[1] PG Scholar

[1] Computer Science & Engineering

[1] Sipna College Of Engineering And Technology,

Amravati, Maharashtra, INDIA

Abstract

In recent years, network-based cyber security attacks have increased in both frequency and intensity, yielding traditional defense practices. as an example, a medium-sized commercial data center network may experience over 100,000 security events per day. These attacks is triggered by a good range of poor performers, from individual hackers to cyber gangs, inciting large organized groups with political or economic motives to cause social disruption.

The development of the web of Things has seen data sharing in the concert of the foremost useful applications in cloud computing. As more this technology has become noticeable, data security is one of the bottlenecks as there are many disadvantages because of misuse of knowledge. during this article, we describe a replacement thanks to secure services by adding a port whitelist to the port whitelist and constantly changing the assignment of services on a port. It aims to cut back the danger of port scanning and unauthorized intrusion attempts and to shield a community of known users from losing data. In short, the port number, time, and IP address are used as a part of the access system; It divides traffic in order that content-based restrictions are often more practical. It also provides connection-based security wrappers for services that are prone to software exploitation, like buffer overruns and backdoors.

Keywords

Cloud Computing, Security Metrics, Security Threats, Security Measurement Frameworks

Introduction

In this project, we are mainly focusing on building a more reliable infrastructure by adding a combination of security concepts for cloud computing in AWS and proposing feasible and available solutions for some of them. Combination of security concepts like multi-factor authentication, key rotation, bastion host, port forwarding, and restricted communication between application hosts. This will help to protect cloud infrastructure from attacks like SQL Injection, DNS Spoofing, and Brute force attacks.

Literature Survey

In October 2015, Patil Madhubala R in her research [1] said that "Firstly computer software was not written considering security as an important factor but due to the increasing frequency of attacks against cloud system newly software include security as a prime concern. Thus, cloud computing is a wide area, so it encompasses so many threats due to its vulnerabilities. We must compromise with one either security or performance. So, Technicians should find a way to build a system that is secure enough for everyday use while possessing reasonable performance and reliable characteristics. It is a big challenge to solve security issues in the cloud."

In March 2017, W. C. N. Kaura and A. Lal, in their survey [2] mentioned, "Cloud computing is the future of computing and storage technology. The exponential increase of connected devices and the need for small and portable devices for complex computation warrant the growth of cloud computing technology. Their paper has discussed cloud technology, various security threats, and prevention measures for ensuring a secure cloud system. The need for security is increasing along with the increasing demand for cloud computing services and the balance must be maintained together."

In December 2019 L. B. Bhajantri and T. Mujawar, in their survey [3] said that "Cloud computing provides a means to store user-sensitive data on cloud servers available in diverse insecure domains. It is necessary to understand and address different security issues in the cloud environment, in order to keep the user's data confidential and protect it against any unauthorized access in the cloud environment. The important aspects of cloud security include proper authentication, a strong encryption technique, and the prevention of data loss. These aspects must be addressed while dealing with all service delivery models and deployment models of the cloud. Their research elaborates on the security concerns present at various levels in the cloud environment. The security measures must be applied to hosts, deployed applications, and networks. While applying security to the data, the proposed security framework should consider data in storage, in transit also traces of deleted data. The proper access control framework is also needed to ensure that only valid users can access cloud resources. The paper addresses various issues,

challenges, and security requirements at each level along with the relevant solutions to mitigate or avoid them."

In 2021 Z. Xiaojian, C. Liandong, F. Jie, W. Xiangqun, and W. Qi, in their research [4] stated that, "The construction of the power Internet of Things has led various terminals to access the corporate network on a large scale. The internal and external business interaction and data exchange are more extensive. The current security protection system is based on border isolation protection. This is difficult to meet the needs of the power Internet of Things connection and open shared services. Their study of the application scheme of the "zero trust" typical business scenario of the power Internet of Things with "Continuous Identity Authentication and Dynamic Access Control" as the core and designs the power internet security protection architecture based on zero trust."

Current System and Lacunas

Traditional IT infrastructures are responsible for protecting data, making it easy for authorized personnel to access stored applications and data. Data centers that are physically connected to the local network can be managed by the internal IT department 24 hours a day, 7 days a week, but it takes a lot of time to ensure that a proper security strategy and data recovery system are in place. It costs money.

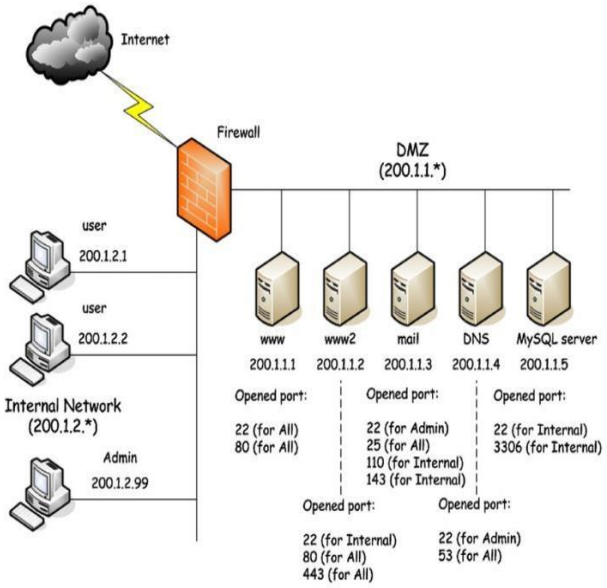

Fig : Traditional networking approach

The cloud is a robust infrastructure that provides reliable and efficient data storage and protection. In terms of external internet threats, when appropriate security measures for preventing and detecting attacks are in place, data in the cloud is no more vulnerable than data stored on any other infrastructure. But the default access control over the internet using a wide range of open ports makes Cloud Infrastructure more vulnerable.

Finding the right solution with strict security cloud services is important to protect the overall security of cloud infrastructure and business. To fill the gaps understood through the analysis, we proposed an access restriction mechanism to the existing cloud infrastructure. The strategy requires meeting specific cybersecurity standards and objectives.

VPC: A virtual private cloud (VPC) could be a secure, isolated private cloud hosted within a public cloud. VPC customers can run code, store data, host websites, and do the rest they may waste a standard private cloud, but the private cloud is hosted remotely by a public cloud provider. (Not all private clouds are hosted during this fashion.) VPCs combines the scalability and convenience of public cloud computing with the information isolation of personal cloud computing.

Imagine a public cloud as a crowded restaurant and a virtual private cloud as a reserved table in this crowded restaurant. although the restaurant is stuffed with people, a table with a "Reserved" register it can only be accessed by the party who made the reservation. Similarly, a public cloud is crowded with various cloud customers accessing computing resources – but a VPC reserves a number of those resources to be used by only 1 customer.

Although a VPC is part of a public cloud, VPCs are logically isolated networks so your data and applications are entirely separate from your provider's other clients. Access is limited to your resources unless you grant this.

Logical isolation makes a VPC environment inherently more secure. However, public cloud security isn't automatic, even with VPC – it must be intentionally deployed.

VPC Security: Cloud security is always a shared responsibility between a cloud provider and its clients. Regardless of the cloud environment, users must take steps to secure data and applications in the cloud. For example, public cloud environments like Amazon AWS can be secured with thirdparty applications that automatically detect and manage threats.

Bastion Host: A bastion host is a computer that is fully exposed to attack. The system is on the public side of the demilitarized zone (DMZ), unprotected by a firewall or filtering router. Frequently the roles of these systems are critical to the network security system. Indeed, the firewalls and routers can be considered bastion hosts. Due to their exposure, a great deal of effort must be put into designing and configuring bastion hosts to minimize the chances of penetration. Other types of bastion hosts include web, mail, DNS, and FTP servers. Some network administrators will also use sacrificial lambs as bastion hosts, these systems are deliberately exposed to potential hackers to both delay and facilitate tracking of attempted break-ins.

Role-Based Access: Improving operational efficiency. With RBAC, companies can decrease the need for paperwork and password changes when they hire new employees or switch the roles of existing employees. RBAC lets organizations quickly add and change roles, as well as implement them across platforms, operating systems (OSes), and applications. It also cuts down on the potential for error when assigning user permissions. Additionally, with RBAC, companies can more easily integrate third-party users into their networks by giving them predefined roles.

Enhancing compliance. Every organization must comply with local, state, and federal regulations. Companies generally prefer to implement RBAC systems to meet the regulatory and statutory requirements for confidentiality and privacy

because executives and IT departments can more effectively manage how the data is accessed and used. This is particularly important for financial institutions and healthcare companies that manage sensitive data.

Giving administrators increased visibility. RBAC gives network administrators and managers more visibility and oversight into the business, while also guaranteeing that authorized users and guests on the system are only given access to what they need to do their jobs.

Reducing costs. By not allowing user access to certain processes and applications, companies may conserve or more costeffectively use resources, such as network bandwidth, memory, and storage.

Decreasing the risk of breaches and data leakage. Implementing RBAC means restricting access to sensitive information, thus reducing the potential for data breaches or data leakage.

Restricted Access: Access Control in cloud security is a system with which a company can regulate and monitor permissions, or access to their business data by formulating various policies suited chosen by the company. Access control in cloud security helps companies gain macro-level visibility into their data and user behavior, which a cloud app may not be able to offer, given their on-demand services and mobility.

Today, data is the most valuable asset of a company, safeguarding it is the next thing to do! Access Control in cloud computing gives companies the control to restrict unauthorized user access and, at the same time, give enough access for smooth functioning at work.

CloudCodes Access Control in cloud security lets companies formulate policies to restrict access through specific IP addresses, browsers, devices, and during specified time shifts. Here's an in-depth view of our Access Control in cloud computing solution.

Conclusion

The key to building a secure network is to define what security means to your need of time and use. Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. It's important to build systems and networks in such a way that the user is not constantly reminded of the security system around him but Users who find security policies and systems too restrictive will find ways around them.

Hence in this project, we have successfully concluded the security policies that can be used, and combined methods so that the multiple is more effective than each component. A bastion host & VPC Architecture along with a port whitelisting makes Cloud infrastructure more redefined.

Reference

[1]. Patil Madhubala R., "Survey on security concerns in Cloud computing," 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), 2015, pp. 1458-1462, doi: 10.1109/ICGCIoT.2015.7380697.

[2]. W. C. N. Kaura and A. Lal, "Survey paper on cloud computing security," 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017, pp. 1-6, doi: 10.1109/ICIIECS.2017.8276134.

[3]. L. B. Bhajantri and T. Mujawar, "A Survey of Cloud Computing Security Challenges, Issues and their Countermeasures," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, pp. 376-380, doi: 10.1109/I-SMAC47947.2019.9032545

[4]. Z. Xiaojian, C. Liandong, F. Jie, W. Xiangqun and W. Qi, "Power IoT security protection architecture based on zero trust framework," 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP), 2021, pp. 166-170, doi: 10.1109/CSP51677.2021.9357607.

[5] W. Zhijun, L. Wenjing, L. Liang and Y. Meng, "Low-Rate DoS Attacks, Detection, Defense, and Challenges: A Survey," in IEEE Access, vol. 8, pp. 43920-43943, 2020, doi: 10.1109/ACCESS.2020.2976609.

[6] Z. Xiaojian, C. Liandong, F. Jie, W. Xiangqun and W. Qi, "Power IoT security protection architecture based on zero trust framework," 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP), 2021, pp. 166-170, doi: 10.1109/CSP51677.2021.9357607.

[7] Yin, S.; Lu, Y.; Li, Y. Design and implementation of IoT centralized management model with linkage policy. In Proceedings of the Third International Conference on Cyberspace Technology (CCT 2015), Beijing, China, 17–18 October 2015; pp. 5–9.

[8] R. Loui, L. Caughey, M. Ghasemisharif and R. Salvador, "Virtualized dynamic port assignment and windowed whitelisting for securing infrastructure servers," 2016 IEEE International Conference on Electro Information Technology (EIT), 2016, pp. 0516-0521, doi: 10.1109/EIT.2016.7535294.

[9] "What is cloud security? - benefits of cloud based security: Box, inc..," Box, 01-Apr-2019. [Online]. Available: https://www.box.com/en-in/resources/whatis-cloudsecurity#:~:text=Cloud%20security%20benefits,recognized%20benefits%20of%20cloud%20computing. [Accessed: 06-Apr-2022].

[10] "What Is Cloud Security? An Introduction | Splunk, 2022" Available: https://www.splunk.com/en_us/datainsider/what-is-cloud-security.html. [Accessed: 06-Apr-2022].