Journal of trends in Computer Science and Smart technology (TCSST) (2020)
Vol.02/ No. 03
Pages: 148-154
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2020.3.004

Study of Security Mechanisms to Create a Secure Cloud in a Virtual Environment with the Support of Cloud Service Providers

S. Stewart Kirubakaran
Assistant Professor
Department of Computer Science and Engineering
Saveetha School of Engineering, Chennai
stewartk.sse@saveetha.com

Abstract: In this paper, we are focussing on creating a secure cloud environment with the help of the cloud service provides. Nowadays, the demand for the cloud increases and all the business are transferred to the cloud environment. When a greater number of people get involved, security matters a lot. This paper emphases on secured cloud environment by creating a trusted relationship with the cloud service provider and also by comparing the current security mechanisms applied in the real-world businesses. This paper helps the readers to understand the need of security mechanisms in the cloud environment and the need for the SLAs with the trusted Cloud Service Providers.

Index Terms: Cloud Security, Cloud Service Providers (CSPs), Service Level Agreement (SLAs), Virtualization, Hypervisor, VMware Workstation

1. Introduction

Cloud Computing is designed with a group of servers that is hosted or implemented on the network to manage and process the data over the internet. It is divided into three types as Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). These above 3 services are combined together to form a cloud computing. The major benefits of Cloud Computing are [Refer Figure 1.1]:

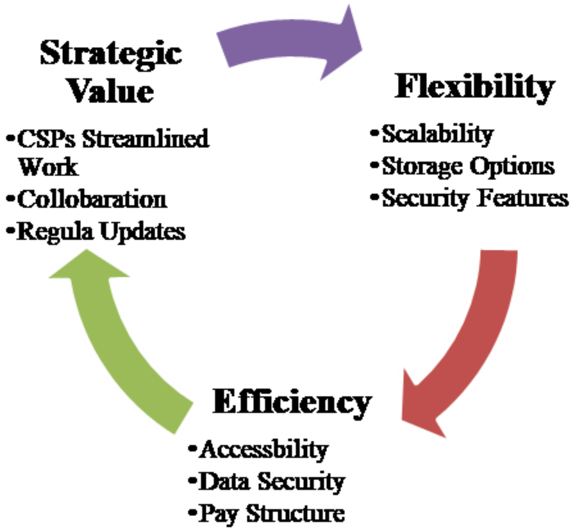

Figure1: Benefits of Cloud Computing [2]

ISSN: 2582-4104
Submitted: 12.06.2020
Accepted: 23.07.2020
Published: 31.07.2020

Cloud Service Providers (CSP) are companies which provides network, storage, computing and security services to the applications in the cloud for businesses applications. It can be accessed by companies or individual with the help of network connectivity. The cloud condition is commonly named as:
Private Cloud – Accessed by an individual organization and its employees
Public Cloud – Can be accessed by anybody in the world via the internet.
Hybrid Cloud – Combination of Private and Public Cloud

2. Cloud Concepts and Technologies

2.1 Load Balancing

It is used to scale up or down the resources available in the cloud environment based on the user needs. There is a threshold limit set to all the servers for incoming user requests. Based on the limit, the scale up or down of resources happens in the network.

2.2 Virtualization

Partitioning the resources of a physical system into multiple virtual resources (such as computing, storage, network and memory) is called as virtualization [1]. It is the main serving technology of cloud computing which allows sharing of networked resources. It helps the users or the customers to meet their demands.

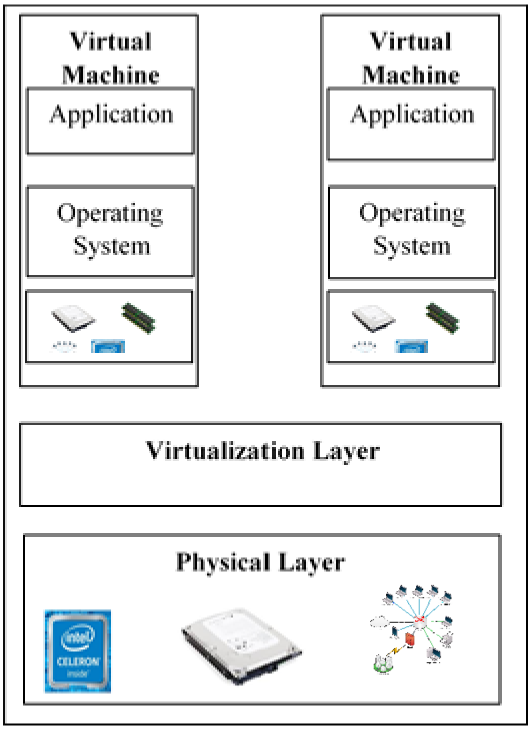

Figure 2.1: Virtualization Layer

2.3 Scalability & Elasticity

The scaling of resources can be classified into two types: Vertical scaling and level scaling. Elasticity is the ability of the system resources to be increased or decreased based on the users requests in an automatic manner through which the demands are met.

ISSN: 2582-4104
Submitted: 12.06.2020
Accepted: 23.07.2020
Published: 31.07.2020

2.4 Service Level Agreements (SLA)

A SLA is an agreement made with the customers based on the services offered to them. The SLAs support service providers to meet the customer expectations.

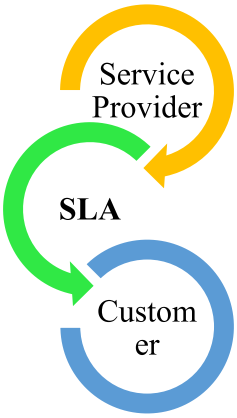

Figure 2.2: Relationship between Service Provider and Customer

3. Cloud Service Providers

3.1 Drop Box

It is best suited for business people where customers don't prefer lot of investments. Some of the main security features of drop box are:

1. 256 bit AES and SSL/TLS Encryption
2. Dropbox Rewind
3. Password-protected and expiring shared links
4. Two Factor Authentication
5. SSO Integrations

3.2 Sophos

It is best suited for educational institutions where customized firewalls can be built. Some of the major security features are:

1. Endpoint protection with AI
2. Firewall with synchronized security built in
3. 24/7 Threat Hunting
4. Secure Web Gateway
5. Anomaly Detection and Analytics

3.3 Google Cloud

It is best suited for people who are google users. Some of the major security features addressed here are:

1. Access Transparency
2. Cloud Key Management Service
3. VPC Security Controls
4. Cloud HSM
5. Secret Manager

3.4 Amazon AWS

It is widely used by all peoples around the world. Some of the major security features are:

1. Identity and Access Management (IAM)
2. S3 Security
3. Cloud Security Groups
4. Vulnerability and Configuration Analysis
5. Security Operations and Automation

ISSN: 2582-4104
Submitted: 12.06.2020
Accepted: 23.07.2020
Published: 31.07.2020

3.5 Microsoft Azure

It provides more security compared to the other cloud providers. Some of them are:

1. Security Center
2. Application Gateway
3. Azure DDoS Protection
4. Key Vault
5. Azure Information Protection

4. Security Algorithms

4.1 RSA

It is the most widely used algorithm. It uses 1024, 2048 and 4096 bits key sizes. NIST Recommends 2048 bit key size for RSA [16]. It follows Asymmetric Encryption process so that two different keys are used.

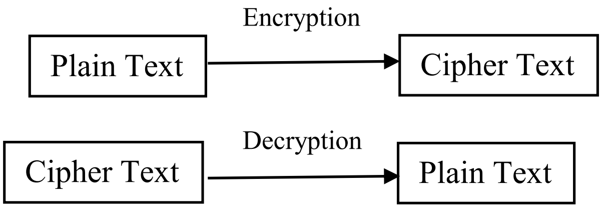

Figure 4.1: RSA Process

4.2 AES

The Advanced Encryption Standard (AES) algorithm is the most widely used algorithm in the market today. Most of the Google Cloud Providers are using it for their day to day demand for the cloud. It uses 256 bit key size. It has been adopted by the US government and is used worldwide by all the organizations [17].

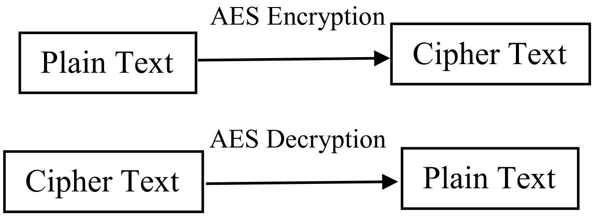

Figure 4.2.1 AES Encryption Process

ISSN: 2582-4104
Submitted: 12.06.2020
Accepted: 23.07.2020
Published: 31.07.2020

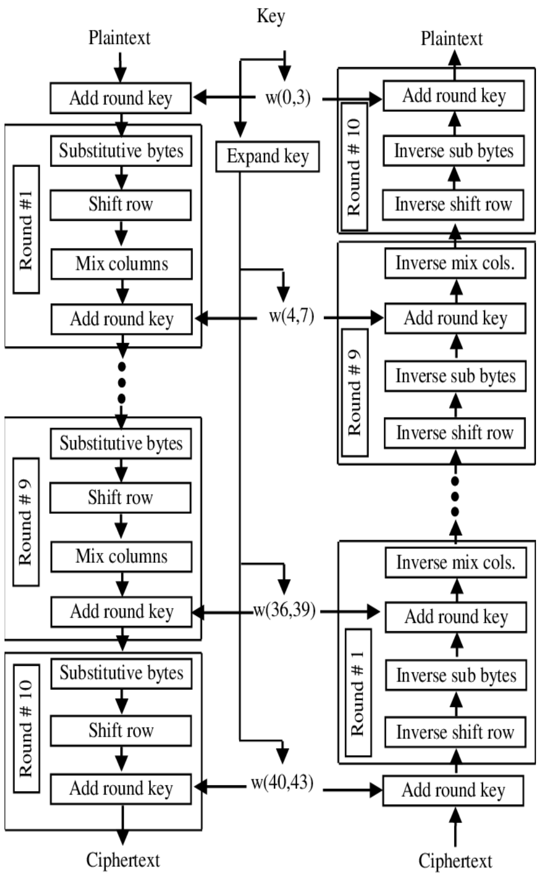

Figure 4.2.2 AES Block Diagram

4.3 DES

The Data Encryption Standard (DES) is a block cipher algorithm that takes plain text as input and converts it into cipher text. It uses symmetric key algorithm for the encryption and decryption process. It uses 64 bits key size.

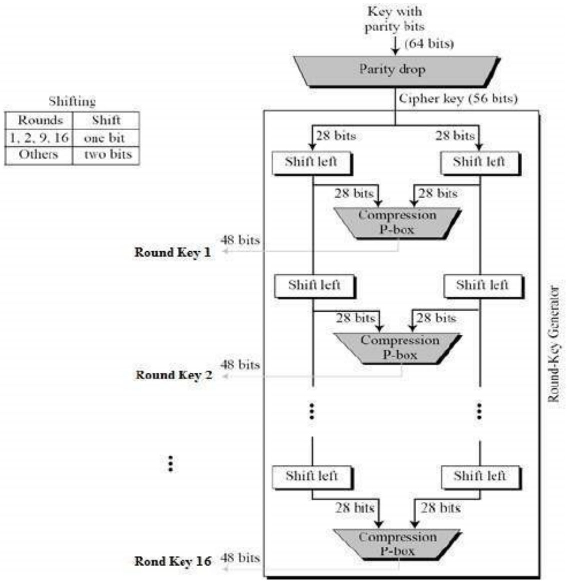

Figure 4.3 Block Diagram of DES

ISSN: 2582-4104
Submitted: 12.06.2020
Accepted: 23.07.2020
Published: 31.07.2020

5. Cloud Security

It is used to protect the data stored in the cloud environment. Some of the Cloud security methods used for protection are

- Firewalls
- Virtual Private Network (VPN)
- Virtualization
- Authorization
- Identity and Access Management
- Authentication

Benefits

Amazon Web Services

- Scale Securely with Superior Visibility and Control
- Automate and Reduce Risk with Deeply Integrated Services
- Build with the Highest Standards for Privacy and Data Security

Google Cloud

- Confidential Computing
- Key Access Justifications
- VPC Service Controls
- Secret Manager

Microsoft Azure

- Start with a secure foundation
- Simplify security with built-in controls
- Detect threats early with unique intelligence
- Key Vault roles

6. Conclusion and Future work

In this paper, we have discussed about the various security mechanisms in the cloud environment and also the impact due to the attacks. It also focuses on the major security features involved in the CSPs like Dropbox, Sophos, Google Cloud, and Amazon AWS. This paper in overall summarizes the existing security features associated with different CSPs and the major attacks that are targeted. This paper helps the researchers to understand the need of security features for the cloud environment and the measures to be taken to enhance the security features associated with the cloud environment.

References:

[1] Cloud Computing a Hands-on Approach by Arshdeep Bahga & Vijay Madisetti published by Universities Press (India) Private Limited 2014.

[2] Benefits of Cloud Computing: https://www.ibm.com/in-en/cloud/learn/benefits-of-cloud-computing

[3] Cloud Service Providers: https://www.sdxcentral.com/cloud/definitions/what-are-cloud-service-providers/

[4] https://blog.turbonomic.com/blog/on-technology/cloud-elasticity-vs-cloud-scalability

[5] https://en.wikipedia.org/wiki/Cloud_computing_security

[6] Sophos Firewall: www.sophos.com

[7] Security Features, IBM: www.ibm.com

[8] https://www.forcepoint.com/cyber-edu/cloud-security

[9] https://www.beyondtrust.com/resources/glossary/cloud-security-cloud-computing-security

[10] https://www.vmware.com/topics/glossary/content/cloud-security

[11] Drop Box Security Features: https://www.dropbox.com/business/plans-comparison

[12] Sophos Tech Specs: https://www.sophos.com/en-us/products/cloud-optix/tech-specs.aspx

[13] Google Cloud Security: https://cloud.google.com/products#security-and-identity

[14] Amazon AWS Security: https://aws.amazon.com/security/

[15] Microsoft Azure Security: https://azure.microsoft.com/en-us/overview/security/

[16] RSA Key Size https://en.wikipedia.org/wiki/Key_size

[17] AES Standards https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

ISSN: 2582-4104
Submitted: 12.06.2020
Accepted: 23.07.2020
Published: 31.07.2020