IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

Secure Cloud Architecture

Prof. Shraddha S. Kulkarni
Department of BBA(CA)
Sarhad College of Arts, Commerce and Science Katraj, Pune, India

Abstract: *Cloud computing refers to the availability of online resources and services. Global data centers serve as the delivery hubs for cloud services. Cloud computing helps its users by giving them access to virtual resources over the internet. Pay-Per Use-On-Demand mode is provided by cloud computing and e-trade. It may be easily accessible and shared via IT resources with the help of the internet. The primary obstacle in cloud computing is to protection and privacy issues arising from its multi-tenancy structure, as well as the outsourcing of critical applications, infrastructure, and sensitive data. Businesses are utilizing cloud services at a rapid pace; therefore, it is necessary to implement measures that ensure businesses have security and can select a provider that suits them. An advancement in current technology that fulfills the long-held dream of computing as a utility is cloud computing. The majority of private and public sector businesses have been deceived by the emergence of this innovative technology in the IT industry.*
The two main security-based approaches now in use for cloud-based platforms are holomorphic encryption and single tamper-proof hardware. Scalability is a problem for hardware-based solutions, but holomorphic encryptions are merely an idea. Furthermore, because of the different nature of its services and deployment strategy, cloud-based platforms cannot directly incorporate standard defense in-depth security mechanisms. To secure the cloud-based platform, however, the same idea of a multi-layered security mechanism can be suggested..

Keywords: Cloud Computer , Saas, Paas, Iaas , Security and Privacy, Threats, Vulnerability

I. INTRODUCTION

Since the term "cloud computing" is becoming more and more common in the information technology (IT) industry, security and accountability have grown in importance. While there are many security problems and worries with cloud computing, they can be divided into two main categories: Security concerns experienced by cloud providers—companies that offer infrastructure, platform, or software as a service—as well as security concerns experienced by its clients. Most of the time, the customer must confirm that the provider has taken the necessary security precautions to protect their information, and the provider must guarantee that their infrastructure is safe and that the data and applications of their clients are protected.

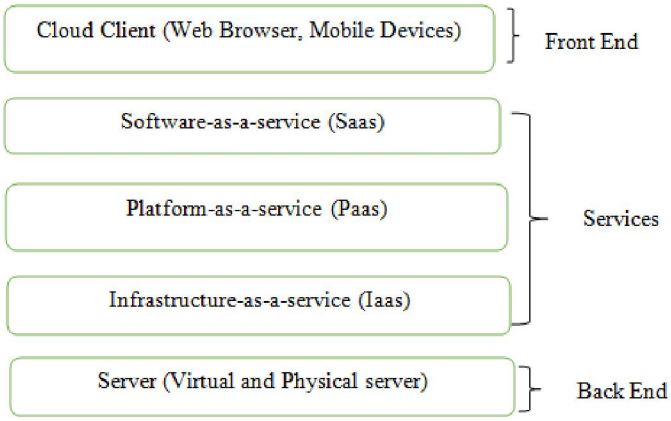

Fig: Cloud Architecture

Figure 1 illustrates how cloud services are provided in terms of Platform-as-a-service (PaaS), Software-as-a-service (SaaS), and Infrastructure-as-a-service (IaaS). It takes a bottom-up strategy, delegating machine power at the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

infrastructure level in terms of memory allocation and CPU utilization. The layer known as PaaS sits on top of it and provides a framework for application development environments. The application layer, located at the top level, provides software that is outsourced over the Internet, doing away with the requirement for complex software to be maintained internally. Application Service Providers (ASPs) can offer software that is hosted remotely to end users at the application layer. Clients do not have to purchase and set up expensive software in this case. Their worries and the cost of usage are within their reach. Cloud computing comprises three delivery models, four deployment models, and five characteristics. These models and characteristics lie on top of each other, forming a cloud stack. The three delivery models of cloud computing environment are: Software-as-a-Service (SaaS). Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). These characteristics help to explain the significance of cloud computing and its adoption. Virtual machines that are available on demand and provide networking infrastructure, computational services, and data storage are known as infrastructure-as-a-service. PaaS is layered on top of IaaS, enabling end users to leverage the resources of their service providers to execute custom applications. Built on top of Platform as a Service (PaaS), SaaS offers business applications that are tailored to a particular use case. Simple multi-tenancy and fine-grained multi-tenancy are the two different forms of SaaS. These deployment methods are positioned at the third tier of a cloud stack. At the top of the cloud stack are five distinct clouds: location-independent resource, transparent network access, on-demand self-service, pooling, rapid elasticity, and regular service.

- **Infrastructure-as-a-service**:- The provision of infrastructure as a service Infrastructure providers oversee a vast array of computational resources, including processing and storage capacity. By virtue of virtualization, they are capable of dividing, allocating, and dynamically resizing these resources to create ad -hoc systems in response to service providers, or customers, requests.
- **Platform-as-a-Service:** Utilizing cloud computing resources, extra abstraction level: they can offer the software in place of a virtualized infrastructure. platform on which systems are operating. The hardware resources required for the services are sized in an open and transparent manner.
- **Software-as-a-service**:-The cloud platform gives developers a transparent, secure, and robust operating and development environment, relieving them of the burden of worrying about the intricacies of managing large-scale servers in the background. Common uses for this paradigm include Force.com, Heroku, Azure, and Google App Engine. Application cloud typically manifests itself as SaaS and directly addresses end software users. Users have the ability to configure, test, assemble, and install every software module in the system.

II. THREATS TO CLOUD COMPUTING

The following are the most prevalent types of cloud-related threats:

Crypto jacking:- While it may be a relatively new type of cyberattack, cryptojacking is also one that can easily slip between the cracks. It revolves around the widely used method of mining cryptocurrency, such as Bitcoin.

Cybercriminals may utilize people's computers, cellphones, tablets, or even servers without permission to mine bitcoin, a practice known as "cryptojacking**."**

Breach of Data

The most frequent danger to cloud computing may be the problem of data breaches leading to leaks or knowledge loss. A knowledge breach usually happens when cybercriminals target a company with the intention of getting unauthorized access to the cloud network or using tools to view, copy, and send data.

Inability to Access

A denial of service (DoS) assault could be one of the biggest risks to cloud computing. These have the ability to overload your cloud services, rendering them inaccessible to your consumers, employees, and business as a whole.

Insider Dangers

When we examine cyber security concerns, we typically picture the thought of hostile criminals breaking into our systems and stealing data - but, sometimes the matter begins from the inner of the corporation . Indeed, according to current figures, insider attacks may be responsible for about 43% of all data breaches.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

III. RISKS RELATING TO CLOUD COMPUTING

Existing risks, vulnerabilities, and related assaults in the cloud create a number of security issues. Vulnerabilities in the Cloud are characterized as gaps in the Cloud's security architecture that an adversary could use with advanced tactics to access the network and other infrastructure resources. The main Cloud-specific vulnerabilities that seriously jeopardize Cloud computing are covered in this section.

Riding in Session and Hijacking

Session hijacking is the use of a legitimate session key to obtain unauthorized access to data or services stored on a computer system. It also refers to the theft of a cookie used for user authentication to a remote server. These terms are related to web application technologies weaknesses in the structure of web applications that allow hackers to carry out a range of malicious activities.

Unsecured Cryptography

Once the primary ways to breach cryptographic mechanisms and algorithms are identified, attackers can decode any of them. Critical vulnerabilities in the implementation of cryptographic algorithms are frequently found and can cause strong encryption to become poor encryption or occasionally not encrypted at all Encryption in any case. For instance, cloud virtualization companies divide servers into images using virtualization software, and then offer those images to users as on-demand services.

IV. REVIEW OF THE WORKS

This review part presents the viewpoints of several writers about current security risks in cloud architecture: Kandukuri, Paturi, and Rakshit (2009) discussed bolstering the Service Level Agreement (SLA) paperwork with a more robust security management commitment. The objectives of this paper are to reduce conflict, simplify complex issues, simplify and identify customer demands, provide a framework for better understanding, encourage communication during disagreements, and avoid setting unreasonably high standards. This document covers the following topics: service definition; performance management; problem management; customer obligations and responsibilities; warranties and remedies; security; disaster recovery and business continuity; and termination policies. This article discussed prior SLA issues with popular waiver programs that might not provide clients with sufficient loss compensation. Consequently, In light of this, the waiver needs to be granted taking into account the business loss and include a number of security guarantees from the cloud provider, such as those on long-term sustainability, regulatory compliance, privilege user access, data placement, and data segregation. One may argue that it's an essential first step in increasing consumer trust in cloud service providers.

Observation:

Examine the observation. The aforementioned assessment pointed out that the three main concepts of security are threats, attacks, and vulnerabilities. Though very few studies concentrate on identifying the sources of these attacks, a large amount of ongoing research seeks to identify attacks and the hazards associated with them. Early vulnerability detection is one strategy to stop threats and attacks, which highlights the significance of establishing a clear link between managing security and identifying different security anomalies. The malevolent phase of Saas services was exploited by the planned risks, vulnerabilities, and assaults, resulting in damage to software and services

Objectives

This aims to uncover security vulnerabilities in cloud computing technologies and provide practical solutions for those vulnerabilities when suitable mitigation strategies have not yet been identified through a survey of the literature. The objective is to identify existing cloud computing security vulnerabilities and their solutions. For problems without mitigating measures, look for solutions, best practices, or instructions from practitioners. Gather these if a challenge has a lot of references but no mitigation techniques.

1) Identify the security problems that cloud computing is currently experiencing and the solutions that have been suggested by the literature.

2) Identify the issues for which there are no known mitigation strategies.

3) Compile business policies, procedures, and fixes for issues where there are more references but no recommended countermeasures.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

4) Provide a list of approaches, guidelines, and fixes for the security vulnerability in cloud computing for which no known mitigating measures exist

Methods:-

Because our research is focused on designing and developing secure and generic architecture (artifacts) for cloud computing platforms, which address common security issues from single domain to multi-domain cloud platform, design science methodology is chosen to achieve the goal of this master's thesis. Several steps comprise our study approach, which are outlined below:

1) Finding security flaws in platforms for cloud computing.
2) Identifying issues and creating a secure architecture.
3) The process involves selecting a suitable open-source cloud platform and closely examining each component of the cloud computing platform. As an example, OpeStack,
4)System study, evaluation, and prototype execution.

Keywords for searches

Constructed research questions served as the basis for the search terms and strings. Additionally, we have provided alternatives and synonyms. We selected synonyms for cloud computing security-related terms from the pertinent literature. The search terms are displayed in the following.

“Cloud Computing”, “Threat”, “ vulnerability”, Iaas, Paas, Saas.

V. CONCLUSION

In the area of security for IT firms, the design and implementation of a general-purpose, safe architecture for cloud computing platforms remains unresolved. Because computing platforms differ in their delivery and deployment methodologies, cloud adoption still requires a generic and safe architecture. The design and implementation of a general and secure architecture for cloud computing platforms is the main goal of this master's thesis. The foundation of the entire design is the idea of service-oriented architecture, which is deployable on any computing platform, independent of the model of delivery and deployment. Our job for testing and deploying central security system design is made easier by OpenStack, an open source platform with a modular architecture. We've talked about the traits of a cloud security system that include vulnerabilities and threats. Businesses that are expanding their on-premise infrastructure to embrace cloud computing should be aware of the security risks associated with this approach. A defense-in-depth strategy must be used to guard against the compromising of the compliance, integrity, and security of their applications and data. Firewall, intrusion detection and prevention, integrity monitoring, log inspection, and virus protection are all part of this line of defense.

REFERENCES

[1]. M. Shaw, D. Garlan, Software Architecture - Perspectives on an Emerging Discipline, Prentice Hall, 1996
[2]. L. Bass, P. Clements, R. Kazman, ‘Software Architecture In Practice’, Addison Wesley,1998
[3]. "Swamp Computing" a.k.a. Cloud Computing". Web Security Journal. 2009-12-28. Retrieved 2010-01-25.
[4]. "Thunderclouds: Managing SOA-Cloud Risk", Philip Wik". Service Technology Magazine. 2011-10. Retrieved 2011-21-21.
[5]. Hassan Takabi and James B.D.Joshi,Security and Privacy Challenges in Cloud Computing Environments, University of Pittsburgh, Gail-Joon Ahn,Arizona State University
[6]. S. Kamara and K. Lauter, "Cryptographic Cloud Storage", FC'10: Proc. 14 Intl.Conf. on Financial, cryptography and data security,2010, pp. 136-149.
[7]. C.L.Li, Z.H. Deng., on the value of cloud computing ,Library and Information , No.4, 2009.
[8]. B. Grobauer, T. Walloschek, and E. Stocker, “Understanding Cloud Computing
[9]. Vulnerabilities,” Security & Privacy, IEEE, vol. 9, no. 2, pp.50-57, 2011.