International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 10, ISSN No. 2455-2143, Pages 96-99
Published Online February 2023 in IJEAST (http://www.ijeast.com)

ESSENTIAL SECURITY DESIGN AND IMPLEMENTATION IN CLOUD COMPUTING

Ramakrishna Subbareddy, Dr. Firdaus Begam
Department of Computer Science
Karpagam Academy of Higher Education, Coimbatore,
India

Abstract— **Cloud computing is a provision structure of online computer service on request and pay per use access to shared resources such as servers, storage, networks, applications, and resources virtual access. Cloud computing is entirely dependent on the internet technology in which client data is stored in data cloud provider center like Google, Amazon and Microsoft etc. This paper presents the computer history of cloud and service models, as well as the security issues and challenges of cloud computing, and discusses cloud computing privacy and explains current laws to protect data and guidelines around the world. Designing a secure virtual cloud path equipment and websites using open-source software (OpenStack) and explain the recommended tips that should always be followed by cloud protection according to the intended categories**

*Keywords-***Virtual Machine, Cloud Computing, Security, Private Cloud, Openstack, IaaS**

I. INTRODUCTION

Computing is a standard model that allows seamless network access, which is essential for a shared collection of configurable computer resources that can be quickly configured and deployed with minimal effort management or collaboration with service providers. The cloud model promotes five key features, three service models, and four application models [8]. The five most important factors are for self-help, extensive network access, integration of resources, fast expansion, and limited service. Three types of service are available in cloud computing such as Infrastructure-as-a-Service (IaaS) Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) called the SPI model It provides a variety of computer services from servers and storage to business applications such as email, security, cache / DR, voice, all delivered online. Value add of the cloud is rapid elasticity: quick scale up and/or down resources and measured service [6] Cloud delivers fast hosting, flexible, secure, and very accessible while saving corporate finance, resources, and time. [1].

II. METHEDOLOGY

There are three service models and four delivery models according to NIST: [10]

- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

The delivery models are:

- Community Cloud
- Public Cloud
- Hybrid Cloud

1. Cloud Computing Main Security Issues:

• **Integrity**: Integrity ensures that the data stored in the system rightly represents the intended data, was not processed by an authorized person. The backup method is configured to be safe in case of data loss, If any application is running on the server. Normally, the data will be backed up to any transferable media that will always be stored off-site. [3].

• **Availability**: Discovery ensures that services of data processing are made available despite malicious conduct. The idea is that when a user attempts to accomplish somewhat, it should be achieved. This is crucial for grave mechanical systems. With the availability of these programs, it is significant for companies to have business continuity plans (BCPs) so that their plans will always work without hindrance. [3]

• **Confidentiality:** It will ensure data doesn’t reach to unauthorized persons. Loss of confidentiality occurs when data can be viewed or read by any unauthorized persons. Loss of privacy can occur physically or electronically. The stealth physical loss occurs through social engineering. When encryptions of connectivity’s in clients and server fails the loss of electronic privacy loss will occur [3].

Confidentiality
Integrity
Availability

Fig. 1. Cloud Computing Security Issues

2. Challenges in Cloud Computing:

The present implementation of cloud computing is related with many challenges since users still doubt its legitimacy. In support of IDC survey in 2008, The following are some of the key encounters that prevent Cloud Computing from actuality accepted by establishments [7]

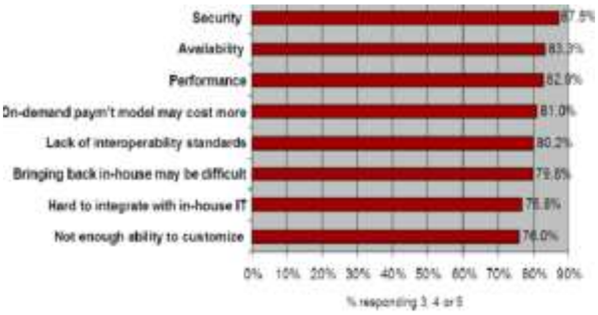

Fig. 2. IDC Survey

A. Security:

The issue of security has played a very imperative role in preventing the adoption of cloud computing. Obviously, using somebody's CPU and having your data on a third-party hard disk seem difficult for several. Security issues like data loss, botnet (remote OS) and identity fraud creates significant threats to software and organizational data. [3]

B. Costing Model:

Cloud buyers need to consider transaction between integration, communication, and calculation [7]. Transitioning to the Cloud can meaningfully reduce infrastructure costs. Apparently, it increases communication costs, i.e., the organizational data transfer cost from the general public therefore there is higher cost per unit of computer equipment used. [4]

C. Charging Model:

The changeable pool of resources makes cost analysis more difficult than conventional data centers that often calculate their costs and support the use of static computing. Additionally, the certified virtual machine has become a price analysis unit rather than a virtual visual server.[4]

D. **Service Level Agreement (SLA):**

Although cloud users haven't any control over basic computer services, they have to confirm the standard, availability, performance and reliability of those services when core business functions of the consumers move into their entrusted cloud. Apparently, consumers should demand assurance for the service delivery from service providers.[4]

E. **What to migrate:**

Based on the IDC (S = = 244) survey shown by IDC in 2008, the seven cloud-based IT systems / applications are: IT Management Applications (26.2%), Personal Applications (25%), Shared Applications (25.4%), Application Development and Delivery (16.8%), Business Applications (23.4%), Storage Capacity (15.5%), and Server Capacity (15.6%). [3]

F. Security for network:

To defend unauthorized access, ill use, computer resources and files hacking securing network are quintessential. Viruses, malware, worms, Identity theft are very common threats to the network. Multilayer security is key feature of network security. Different programs to be used for different threats. Network security measures are very much needed to protect data during their transmission, between end user and computer and between peer computers [5]

G. Data Location:

Customers might not recognize the precise location of the server used to store and process their applications and data. Cloud computing technology lets cloud servers to be hosted anyplace worldwide. From a technical standpoint, space is typically not functional.

H. Data Protection:

The data is stored in a shared cloud space i.e. in a shared location it is accessed by another client's data. The types of data stored in the cloud can also vary to keep data away from controlling access for unauthorized users and encryption end options [11]

I. Identity and Access Management:

Managing your identity and managing access to business applications remain a major challenge for IT today. While an enterprise may be able to use a few cloud computing services without proper ownership and access control strategy, long-term expansion of the organization's ID services in the cloud is a necessary requirement for the implementation of the required computer resources

J. Backup and Recovery issues:

Cloud Computing servers are a place where users store all sensitive business data. A standard backup copy of user data needs to be created as an error-free solution and restored to a disaster situation when the original data is gone [12].

III. APPROACH EFFECT

OpenStack is a cloud-based OS that manages large amounts of data, storage, and communication resources across the data center, managed with a dashboard that gives controllers while giving their users the ability to provide services through web-based interface.

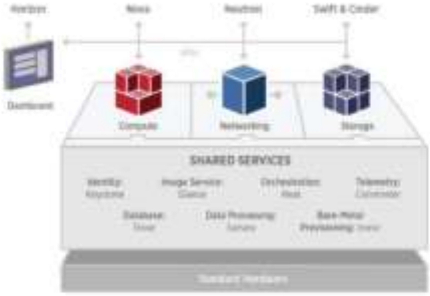

Fig. 3. Architecture of Openstack

Network Side

•To manage the network in the virtual environment OVS (Open VSwitch) has been used in all Servers

• we separated the network traffic by using Bridge and port technology in OVS

• We used two interfaces to produce internal and external connectivity in network service (Neutron)

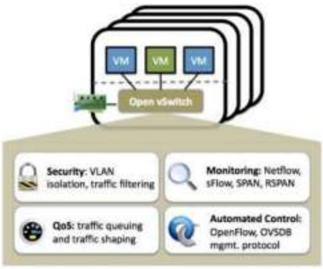
VM
VM
VM
Open vSwitch
Security: VLAN isolation, traffic filtering
Monitoring: Netflow, sFlow, SPAN, RSPAN
QoS: traffic queuing and traffic shaping
Automated Control: OpenFlow, OVSDB mgmt. protocol

Fig. 4. OVS Features

Compute Node Side

• To support creating virtual machines we installed Nova Service (in OpenStack)

• we used KVM (Kernel-based Virtual Machine) technology In Hypervisor to make the visualization.

• Created multi node as a clustering to realize High Availability (HA).

• used IP tables technology to provide security for hypervisor.

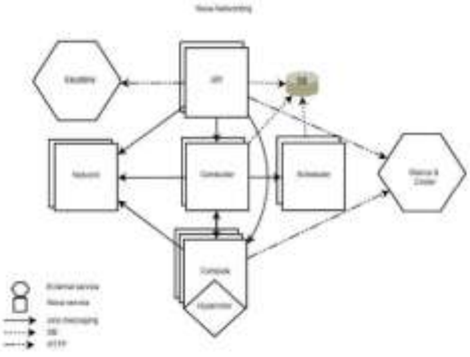

Fig. 5. NOVA Design

IV. CONCLUTIONS AND RECOMMENDATIONS

In this paper we have conversed computer cloud security challenges and issues, computer computing privacy and devised a way to work on all confidential clouds using OpenStack software. Cloud computing is a contemporary technology and hence need to consider lot of issues. Cloud has many sweeping issues and among technical issues including flexibility, durability, reliability, licensing software, ownership, system development and data management and non-technical issues as part of legal and economic. Cloud computing still a risky and many challenges may arise, and solutions must be developed to form this technology work proficiently. So, this research does not end here with a lot of work that could be accomplished in the future. The design model presented in this study stands first step and entails further tuning; yet it can provide the foundation for in-depth learning on the privacy and security of cloud computing to the research community occupied in the turf of Cloud Computing. For future job research the following steps are recommend that you to ensure that you protect the cloud:

Install and save firewall configuration. The firewall must be located in the interface of each external network and within each security area within the cloud.

- Do not use the dealer provided passwords and other security restrictions.
- Research into standard SLAs and credit providers can lead to greater accountability.
- Make sure there are no unnecessary tasks or processes in place and active.
- Make sure patch management is done periodically.
- Ensure Encryption keys are protected from misuse or disclosure

V. REFERENCE

[1]. C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser. “Business Models in the Service World.”IT Professional, vol. 11, pp. 28-33, 2009.

[2]. Peter Mell Timothy Grance, “The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology”.

[3]. F. Gens., “New IDC IT Cloud Services Survey: Top Benefits and Challenges”, IDC exchange, Available: Feb. 18, 2010

[4]. Cataline Negru, Valentin Cristia “Cost models-pillars for efficient cloud computing: Position paper: July 2013

[5]. L. Ertaul, S. Singhal, and G. Saldamli,” Security Challenges in Cloud Computing”

[6]. Ashish Kumar “Cloud Computing Challenges”: A Survey: October 201

[7]. Tharam Dillon, Chen Wu, Elizabeth Chang “Cloud Computing: Issues and Challenges” 2010

[8]. Amin Jula, Elankovan Sundararajan, Zalinda Othman,” Cloud computing service composition: A systematic literature review”,2014,3

[9]. Mohamed Ismail, Ashraf GasimElsid, “Design and Implementation of Cloud Computing Security and Privacy System” September 2017

[10]. Evaluation of Cloud Computing Services Based on NIST SP 800-145, 2018

[11]. D. Zissis et al. “Addressing cloud computing security issues” Future Gener Computer Systems (2012)

[12]. R. Bhadauria et al. “Survey on security issues in Cloud Computing and Associated Mitigation Techniques” International Journal of Computer Applications (0975-888) (June 2012)