IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 11, November 2021

DOI: 10.17148/IARJSET.2021.81143

Security Framework for Cloud Computing

Sabugar Mohmadfurkan[1], Asst.Prof Jinal Patel[2]

Student of M.E, Computer Engineering Dept, Grow More Faculty of Engineering, Himmatnagar, Gujarat, India[1]

Grow More Faculty of Engineering, Udaipur – Himmatnagar Highway, Himmatnagar, Gujarat, India[2]

Abstract: Cloud computing is one of the huge things in data innovation and in information technology world. cloud computing give boundless foundation or infrastructure to storage or running client's information/software. Cloud computing is a since quite a while ago envisioned vision of figuring as a utility, where information owner can remotely store their information in the cloud to appreciate on-requestprofoundly quality application and services from a mutual configurable registering assets. Our paper gives cloud computing security issue and ways to deal with secure the information. Our proposed framework we expect will be more secure, to addressing forensic computing in cloud computing as one of the most important emerging issues and highlighted security challenges.

Keywords: Attack, Pubic Cloud, Cloud Computing, Security

I. INTRODUCTION

This Cloud computing allow to both the applications delivered as services over the Internet and the equipment(hardware) and frameworks(software system) in the server or data centre that give those services. Cloud computing is as of now rising as a component for high level or professional, and in addition filling in as a storage framework system for assets (resources).Cloud enable clients to pay for whatever assets they utilize, enabling clients to increment the amount of assets as required needed [10]. This new computing paradigm is referred as a cloud computing. In this paper will describe a general structure of cloud computing in which the application and regularly the information itself is stored directly not on your pc but rather a remote server that is associated with the internet. Here focus on the structure of a cloud in which the cloud utilizes the various application, for example, Amazon, Google applications for storing the data [9].

Type Of Cloud Commuting Mode

For secure services in cloud computing there are two kind of model. Initially is the delivery model and another is deployment model.

Delivery model: Delivery model in cloud computing we characterize and define by the three keys that are infrastructure as a service (IaaS), Software as a service (SaaS), Platform as a service (Paas) see (figure1).

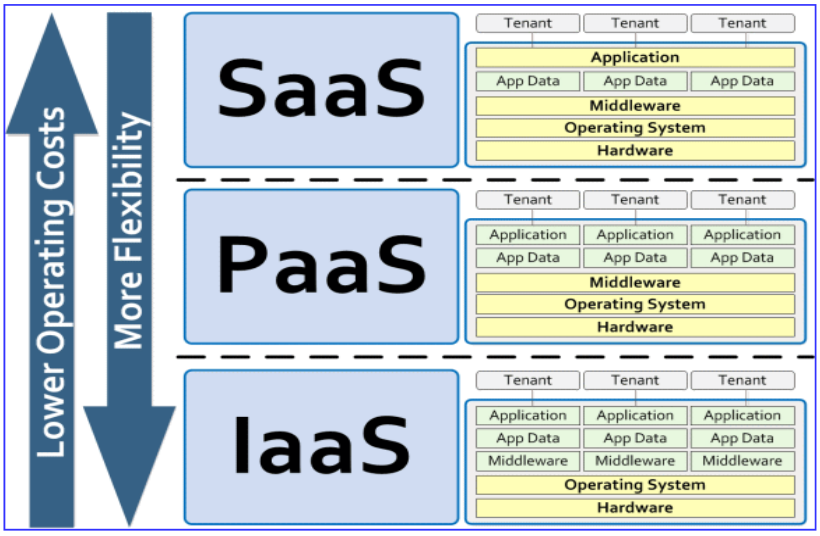

Figure1: Delivery Model

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 11, November 2021
DOI: 10.17148/IARJSET.2021.81143

Infrastructure as services (Iaas) is the establishment of all the cloud services (bottom layer). It supplies an arrangement of virtualized infrastructural segment, for example, virtual machines. Platform as services (Paas) is a centre layer in cloud services. It enables programming environment to access and use extra application building block. Software as a services (Saas) works on the virtualized and pay-per-utilize costing model whereby software applications are rented out to contracted association by specific or specialized saas merchant (vendor) [9].

Deployment model:

- **Public Clouds:** In public cloud, the services and infrastructure are given off-site over the Internet. These clouds offer the best level of effectiveness in shared recourses (assets); however, they are less secured and vulnerable rather than private clouds.
- **Private Clouds:** Differ from public clouds, in the Private Clouds, the services and infrastructure are kept up and maintained on a private system network. These clouds offer the best level of security and control. However, they require the organization to in any case buy and keep up all the product (software) and infrastructure(framework).
- **Hybrid Clouds:** Hybrid cloud incorporates a variety of public and private choices with different suppliers orprovider.
- **Community Clouds:** A Community cloud in computing is a collaborative effort in which infrastructure is shared between several organization from a specific community with common concerns.

In basic terms, when you are utilizing cloud computing, you do not have to introduce and install the required application on your framework system. Rather, you utilize the application that keeps running on a remote area, which we called the 'Cloud 'see (figure2).

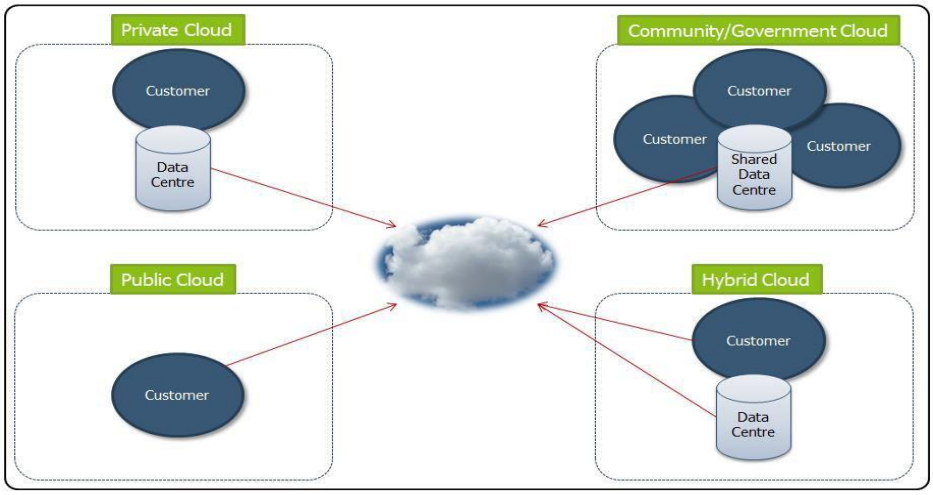

Figure2: Deployment Model

After learning about the cloud and its types, we present the most important challenges facing in cloud computing:

- **Decentralization of server farms:**

Distributed computing's conveyed design enables information to be made, put away, handled and appropriated more than a few server farms and physical machines which are universally scattered and furthermore conceivably scattered into different topographical areas and purviews. Information is reproduced to different servers to guarantee excess of information.

- **Reliance on CSP In a distributed computing condition:**

The cloud specialist co-op has all the control over the earth and hence controls the wellspring of the evidential information. The way toward safeguarding advanced proof in the cloud very relies upon the help that the examiner gets from the cloud specialist co-op (CSP).

- **Metadata/Provenance security:**

Metadata, otherwise called information provenance, is the historical backdrop of advanced items. Metadata depicts possession and the procedure history (make, adjust and access) of information objects. Metadata is crucial to the accomplishment of measurable examinations with a specific end goal to decide the responsibility for information (who get to the information) and the course of events of evidential information (when information got to)

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 11, November 2021

DOI: 10.17148/IARJSET.2021.81143

II. LITRITURE REVIEW

- **"A survey on security issues in service delivery models of cloud computing "** Over the most recentyears, cloud computing has developed from being a promising business idea to one of the fast developing portions of the IT business .Despite of all buildup encompassing the cloud ,enterprise client are still send their business in the cloud. Security is one of the real issues which restrict the development of cloud computing and complications with information security, privacy and information protection keep on plaguing the market [1].
- **"Quirc: A quantitative impact and risk assessment framework for cloud security "** Six key Security Objectives (SO) are distinguished for cloud stages, and it is suggested that a large portion of the run of the millassault vectors and occasions guide to one of these six classes. Wide-band Delphi strategy is proposed as a logical intends to gather the data essential for surveying security dangers. Chance appraisal knowledgebase could be created particular to every industry vertical, which then fill in as contributions for security hazard evaluation of cloud computing stages. QUIRC's key leeway is its completely quantitative and iterative union approach, which empowers partners to nearly survey the relative strength of various cloud merchant offerings and methodologies in a solid way [2].
- **"The management of security in cloud computing "** cloud computing has raised IT to more up as far as possible by offering the market environment information storage and limit with adaptable versatile registering handling energy to match flexible request and supply, while decreasing capital consumption. However the opportunity cost of the fruitful usage of Cloud computing is to viably deal with the security in the cloud applications. Security awareness and concerns emerge when one starts to run applications past the assigned firewall and towards public domain [3].
- **"Personal cloud computing security framework "** cloud computing is a developing term nowadays. It display the progress of many existing IT advancements and isolates application and data assets from the fundamental foundation. Personal Cloud is the hybrid deployment model that is combined private cloud and public cloud. Largely, cloud orchestration does not exist today. Web browser provides current cloud service or host installed application directly. As indicated by the ITU-T draft, we should seriously mull over cloud coordination environment in a joint effort with other cloud suppliers. Previous work [4].
- **"Collaboration-based cloud computing security management framework "** The cloud computing model display to another paradigm change in web based services that delivers professional distributed computing platforms in which computational resources are offered 'as a service'. Despite the fact that the cloud model is intendedand designed to receive uncountable rewards for all cloud partners including cloud suppliers (CPs), cloud customers (CCs), and services provider (SPs), the model still has various open issues that affect its validity[5].
- **"Security framework for cloud computing environment: A review "**

Cloud computing has an extensive variety of properties some of which are as the following:-

- **Shared Infrastructure:** cloud condition utilizes a powerful software model that permits sharing of physical services, storage and networking capabilities among clients. The cloud foundation infrastructure is to discover the vast majority of the accessible infrastructure over multiple clients .
- **Network Access:** Cloud services are accessed to over a network system from an extensive variety of devices, for example, PCs, tablets, and cell phones by utilizing measures based APIs .
- **Handle Metering:** Cloud services provider or partner store data of their customers for managing or handling and enhancement the services and to give revealing or reporting and charging data. Because this, clients are payable for services as per the amount they have really utilized among the charging or billing period[6].

III. METHODOLOGY

Cloud computing has become a changing platform for organizations to create their infrastructure and frameworks. If organizations are to consider using cloud-based systems, they will face the task of reassessing their current security strategy.

Methodology In this paper:

1. Describe the recent papers published in 2015-2020 on the risks and security issues faced by organizations using cloud computing in their dealings and some proposed or recommended solutions to avoid those risks and then discuss their applicability.

2 - The most usedfull methods help to avoid the security risks facing in the cloud computing.

3 - Proposing a curriculum that combines all the advantages and takes advantage of the capabilities of the previous curricula in solving the challenges and security issues and adding many characteristics and features that make it an integrated approach to enhance the security aspect

4 - Add solutions proposed for the most prominent challenges in the field of forensic medicine in the cloud computing.

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 11, November 2021

DOI: 10.17148/IARJSET.2021.81143

5. Writing future proposals on the curriculum and presenting the main obstacles faced by the researcher.

IV. CONCLUSION

In this proposed research we review the concept of cloud computing and its components and different types. The research also examined the difference between current cloud computing models and the gaps affecting cloud computing work and effectiveness. One of the most important problems for this type of high-risk technology is security challenges. We highlighted many different security challenges and problems, proposed solutions to the solution as well as providing a proposed framework that enhances the security aspect.

Our proposed framework is expected to be more secure, in addition to addressing criminal computing in cloud computing as one of the most important emerging issues, and emerging security challenges.

REFERENCES

[1]. Subashini, Subashini & Kavitha, Veeraruna (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34, 1-11.

[2]. Saripalli, Prasad& Walters, Ben(2010). Quirc: A quantitative impact and risk assessment framework for cloud security. Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on,280-288.

[3]. Ramgovind, Sumant & Eloff, Mariki (2010). The management of security in cloud computing. Information Security for South Africa (ISSA), 2010,1-7.

[4]. Sang-Ho a, Park& Jun-Young , Huh(2010). Personal cloud computing security framework. Services Computing Conference (APSCC), 2010 IEEE Asia-Pacific,671-675.

[5]. Almorsy, Mohemed & Grundy, John(2011). Collaboration-based cloud computing security management framework. Cloud Computing (CLOUD), 2011 IEEE International Conference on,364-371.

[6]. Malik, Ayesha & Nazir, Muhammad(2012). Security framework for cloud computing environment: A review. Journal of Emerging Trends in Computing and Information Sciences,390-394

[7]. Brodkin, Jon(2008). Gartner: Seven cloud-computing security risks, Infoworld,1-3.

[8]. Sharma, Sanjana & Soni, Sonika(2012). Security in cloud computing. National Conference on Security Issues in Network Technologies [9]. Armbrust, Michael &Fox, Armando(2010). A view of cloud computing. Communications of the ACM,50-58.

[10]. Zunnurhain, Kazi & Vrbsky, Susan(2011). Security in cloud computing. Proceedings of the 2011 International Conf on Security \& Managemt. [11]. P. Gladyshev, A. Marrington, "Digital Forensics and Cyber Crime", First International Conference ICDF2C 2013, 2009.

[12]. P. Gladyshev, A. Marrington, "Digital Forensics and Cyber Crime", First International Conference ICDF2C 2013, 2009.

[13]. G. Meyer and A. Stander, "Cloud Computing: The Digital Forensics Challenge", in Proceedings of Informing Science & IT Education Conference, 2015, pp. 285-299.

[14]. Khan S, Gani A, Abdul Wahab AW, Shiraz M, Bagiwa MA, Khan SU, Buyya RK, Zomaya AY, Cloud Log Forensics: Foundations, State-of-the-art, and Future Directions, ACM Computing Surveys. 2016b. (In Press).

[15]. Thorpe, I. Ray, T. Grandison, and A. Barbir. 2012a. Cloud log forensics metadata analysis. In Proceedings of the IEEE Computer Software and Applications Conference Workshops (COMPSACW). 194-199.