e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:11/November-2023 Impact Factor- 7.868 www.irjmets.com

REASEARCH IN CLOUD COMPUTING

Ganesh Patole*1

*1B.Sc Information Technology, B.K. Birla College, Kalyan, Maharashtra, India.

DOI : https://www.doi.org/10.56726/IRJMETS45855

ABSTRACT

"Cloud" is a collective term for a large number of developments and possibilities. It is not an invention, but more of a "practical innovation", combining several earlier inventions into something new and compelling. Much like the iPod is comprised of several existing concepts and technologies (the Walkman, MP3 compression and a portable hard disk), cloud computing merges several already available technologies: high bandwidth networks, virtualization, Web 2.0 interactivity, time sharing, and browser interfaces. Cloud Computing is a popular phrase that is shorthand for applications that were developed to be rich Internet applications that run on the Internet (or "Cloud"). Cloud computing enables tasks to be assigned to a combination of software and services over a network. This network of servers is the cloud. Cloud computing can help businesses transform their existing server infrastructures into dynamic environments, expanding and reducing server capacity depending on their requirements. A cloud computing platform dynamically provisions, configures, reconfigures, and deprovisions servers as needed. Servers in the cloud can be physical machines or virtual machines.

I. INTRODUCTION

In today's era every organization wants to implement Cloud Computing to fullfil their needs of computing. The

Cloud computing is a fastest growing area in every sector like IT industry government organizations etc. The Cloud computing emerges as a new computing paradigm which aims to provide computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. The intent of this paper is to have a review on cloud computing, its working ,its use in various sectors, deployment models and services. The word "cloud" refers to flowcharts that historically represented the infrastructure of the internet as a cloud-like shape. Clouds were used to simplify network diagrams. The cloud icon implied that the underlying structure of the internet wasn't relevant to an application. Similarly, with cloud computing, the systems that support the cloud resources (notably the physical hardware) do not matter to the end user.

Cloud computing is available in several models:

Infrastructure-as-a-Service (IaaS) model that provides low-level, fine-grained control of computational resources; and

Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) solutions, which offer valuable, simplifying abstractions, but are less flexible.

II. CLOUD COMPUTING MODELS

Cloud hosting deployment models are classified by the proprietorship, size and access. It tells about the nature of the cloud. Most of the organizations are willing to implement cloud since it reduces the expenditure and controls cost of operation

Cloud computing deployment models

A.) Public Cloud.

Organizations can also opt for a storage-as-a-service provider in the public cloud. The provider delivers a storage platform with offerings such as bare-metal storage capacity, object storage, file storage, block storage and storage applications like backup and archiving.

Public cloud is an alternative deployment approach to traditional on-premises IT architectures. In the basic public cloud computing model, a third-party provider hosts scalable, on-demand IT resources and delivers them to users over a network connection, either over the public internet or a dedicated network. Public cloud computing is often viewed as utility computing, where computing capabilities are delivered to users on demand, just as any other utility, such as water, gas and telecommunications.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:11/November-2023 Impact Factor- 7.868 www.irjmets.com

B. Private Cloud

A third-party cloud service provider manages the underlying computing resources. The provider is responsible for resource maintenance and guarantees availability, reliability, and security through servicelevel agreements. You don't buy, own, and maintain physical data centers and servers; instead, you access technology services on an as-needed basis. In addition, several tasks, such as runtime resource scaling, are automated for operational efficiency.

Private cloud compared to public cloud

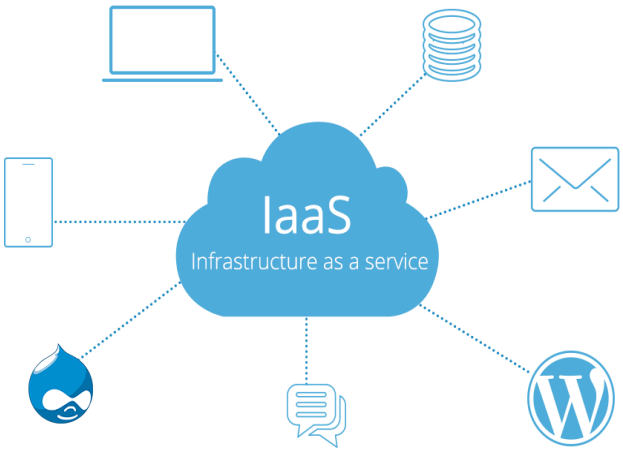
It is almost impossible to replicate public cloud infrastructure privately. You get significantly more breadth and depth of services from a public cloud provider because it is fully dedicated to scaling and improving its offerings. You also get more innovation, access to a global community, and proven operational expertise.

C. Hybrid Cloud

A hybrid cloud is a mixed computing environment where applications are run using a combination of computing, storage, and services in different environments—public clouds and private clouds, including onpremises data centers or "edge" locations. Hybrid cloud computing approaches are widespread because almost no one today relies entirely on a single public cloud.

Hybrid cloud solutions enable you to migrate and manage workloads between these various cloud environments, allowing you to create more versatile setups based on your specific business needs. Many organizations choose to adopt hybrid cloud platforms to reduce costs, minimize risk, and extend their existing capabilities to support digital transformation efforts.

A hybrid cloud approach is one of the most common infrastructure setups today. Cloud migrations often naturally lead to hybrid cloud implementations as organizations often have to transition applications and data slowly and systematically. Hybrid cloud environments allow you to continue using on-premises services while taking advantage of the flexible options for storing and accessing data and applications offered by public cloud providers, such as Google Cloud.



D. Community Cloud

A community cloud is a cloud infrastructure in which multiple organizations share resources and services based on common operational and regulatory requirements. The concept of a community cloud is akin to a community garden, where different individuals grow produce on a single piece of shared land. Community clouds are a recent phenomenon compared to other cloud models such as public, private, and hybrid clouds.

The COVID-19 pandemic has pushed the world to embrace a remote work setup across industry verticals. It has left sectors such as education and healthcare scrambling to move completely online, which they were not ready for. This accelerated cloud adoption, with Gartner predicting that worldwide public cloud adoption will increase by 18% in 2021.

High costs mean that a private cloud is, more often than not, out of reach for many small organizations, while industry regulations make public cloud unfeasible for many others. This is where community cloud comes into

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:11/November-2023 Impact Factor- 7.868 www.irjmets.com

the picture. This system is a modified form of private cloud, where the needs of different organizations and verticals are weighed during architecture ideation. A community cloud system is owned, managed, and operated by members of the community, third-party vendors, or both.

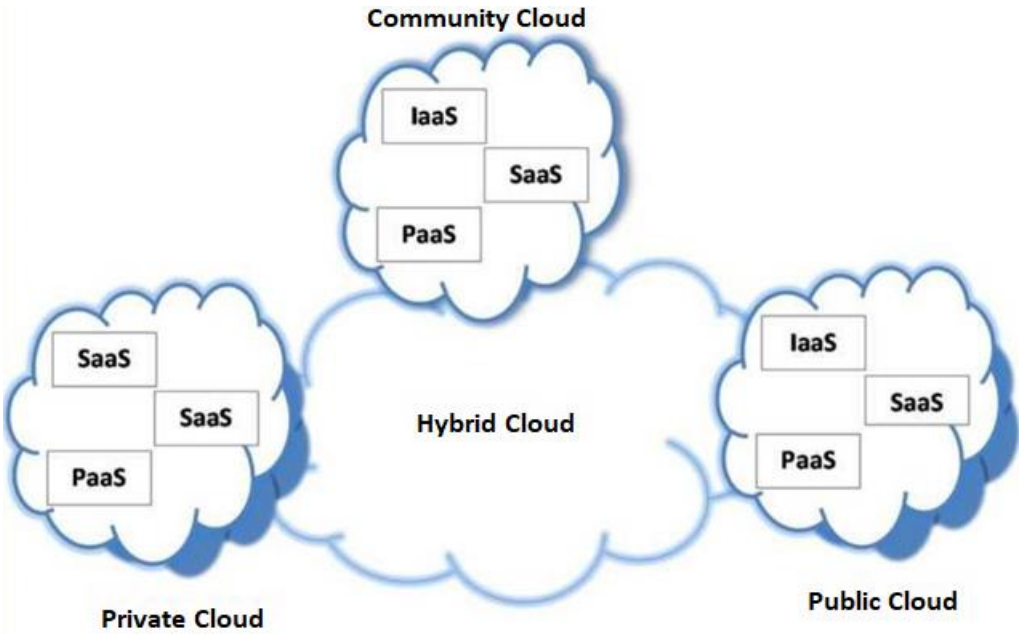
III. CLOUD SERVICE MODELS:

Software as a Service (SaaS)

Software as a Service (SaaS) is growing rapidly. SaaS makes uses the web to provide applications which are managed by a third-party vendor and whose interface is accessed on the client side. SaaS applications can be run from a web browser without the need to download or installation, but these require plugins. The cloud provider provides the consumer with the ability to deploy an application on a cloud infrastructure [5]. Because of this web delivery model SaaS removes the need to install and run applications on individual computers. In this model it is easy for enterprises to improve their maintenance and support, because everything can be managed by vendors: applications, runtime, data, middle ware. OS, virtualization, servers, storage and networking. Popular SaaS services include email and collaboration, healthcare-related application. SaaS providers usually offer browser-based interfaces. APIs are also normally made available for developers. The key benefit of SaaS is that it requires no advance investment in servers or licensing of software. The application developer, have to maintain one application for multiple clients.

Infrastructure as a Service (IaaS)

Infrastructure as a Service, are used for monitoring, and managing remote datacenter infrastructures, such as compute (virtualized or bare metal), storage, Users can purchase IaaS based on consumption, similar to other utility billing. IaaS users have the responsibility to be in charge applications, data, runtime and middleware.. Providers can still manage virtualization, servers, storage, and networking. IaaS providers offer databases, messaging queues, and other services above the virtualization layer as well.



Platform as a Service (PaaS)

Platform as a Service, also known as PaaS, is a type of cloud computing service model that offers a flexible, scalable cloud platform to develop, deploy, run, and manage apps. PaaS provides everything developers need for application development without the headaches of updating the operating system and development tools or maintaining hardware. Instead, the entire PaaS environment—or platform—is delivered by a third-party service provider via the cloud.

PaaS helps businesses avoid the hassle and cost of installing hardware or software to develop or host new custom applications. Development teams simply purchase pay-as-you-go access to everything they need to build custom apps, including infrastructure, development tools, operating systems, and more.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:11/November-2023 Impact Factor- 7.868 www.irjmets.com

The result is simpler, faster, and secure app development that gives developers the freedom to focus on their application code.

IV. SECURITY ISSUES

Cloud service models not only provide different types of services to users but they also reveal information which adds to security issues and risks of cloud computing systems. IaaS which is located in the bottom layer, which directly provides the most powerful functionality of an entire cloud.

IaaS also enables hackers to perform attacks, e.g. brute-forcing cracking, that need high computing power. Multiple virtual machines are supported by IaaS, gives an ideal platform for hackers to launch attacks that require a large number of attacking instances. Loss of data is another security risk of cloud models.

Data in cloud models can be easily accessed by unauthorized internal employees, as well as external hackers. The internal employees caneasily access data intentionally or accidently. External hackers may gain access to databases in such environments using hacking techniques like session hijacking and network channel eavesdropping. Virus and Trojan can be uploaded to cloud systems and can cause damage [6]. It is important to identify the possible cloud threats in order to implement a system which has better security mechanisms to protect cloud computing environments.

Threats in cloud computing

A. Compromised credentials and broken authentication

Organizations/companies at times struggle with identity management as they try to grant permissions appropriate to the user's job role. They sometimes forget to remove user access when a job function changes or a user leaves the organization. The Anthem breach exposed more than 80 million customer records, was the result of stolen user credentials. Anthem had failed to deploy multifactor authentication, so when the attackers obtained the credentials, it was all over. Many developers have made the mistake of embedding credentials and cryptographic keys in source code and have them in public-facing repositories .

B. Data breaches

Cloud environments face many of the same threats as traditional corporate networks, but since a large amount of data is stored on cloud servers, providers have become an attractive target. The severity of the damage tends to depend on the sensitivity of the data that is exposed. Personal financial information grabs the headlines, but breaches involving government information, tradesecrets can be more devastating. When a data breach takes place, a company may be subjected to legal action. Breach investigations and customer notifications can rack up significant costs. Indirect effects may include brand damage and loss of business can impact organizations future for years.

C. Hacked interfaces and APIs

Today every cloud service and application now offers APIs. IT teams use these interfaces and APIs to manage networking. Popular SaaS services include email and collaboration, healthcare-related application. SaaS

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:11/November-2023 Impact Factor- 7.868 www.irjmets.com

providers usually offer browser-based interfaces. APIs are also normally made available for developers. The key benefit of SaaS is that it requires no advance investment in servers or licensing of software. The application developer, have to maintain one application for multiple clients.

Infrastructureasa Service (IaaS)

Infrastructure as a Service, are used for monitoring, and managing remote datacenter infrastructures, such as compute (virtualized or bare metal), storage, Users can purchase IaaS based on consumption, similar to other utility billing. IaaS users have the responsibility to be in charge applications, data, runtime and middleware.. Providers can still manage virtualization, servers, storage, and networking. IaaS providers offer databases, messaging queues, and other services above the virtualization layer as well.

Platform as a Service (PaaS)

SECURITY ISSUES

Cloud service models not only provide different types of services to users but they also reveal information which adds to security issues and risks of cloud computing systems. IaaS which is located in the bottom layer, which directly provides the most powerful functionality of an entire cloud.

IaaS also enables hackers to perform attacks, e.g. brute-forcing cracking, that need high computing power. Multiple virtual machines are supported by IaaS, gives an ideal platform for hackers to launch attacks that require a large number of attacking instances. Loss of data is another security risk of cloud models.

Data in cloud models can be easily accessed by unauthorized internal employees, as well as external hackers. The internal employees caneasily access data intentionally or accidently. External hackers may gain access to databases in such environments using hacking techniques like session hijacking and network channel eavesdropping. Virus and Trojan can be uploaded to cloud systems and can cause damage [6]. It is important to identify the possible cloud threats in order to implement a system which has better security mechanisms to protect cloud computing environments.

Browser Security

Client uses browser to send the information on network. These browsers use SSL technology to encrypt user's identity and credentials. But hackers from the intermediary host may obtain these credentials by using sniffing packages installed on the intermediary host. One should have a single identity but this credential must allow different levels of assurance which can be achieved by obtaining approvals digitally.

V. CONCLUSION

Cloud Computing is a new concept that presents quite a number of benefits for its users. But it also raises some security problems which may affect its usage. Understanding about the vulnerabilities existing in Cloud Computing will help organizations to make the shift towards using the Cloud. Since Cloud Computing leverages many technologies and it also inherits their security issues. Traditional web applications, virtualizations have been looked over but some of the solutions offered by cloud are immature or inexistent. We have presented security issues for cloud models: IaaS, PaaS, and IaaS, which differ depending on the model. As described in this paper, storage and networks are the biggest security concerns in Cloud Computing. Virtualization that allows multiple users to share a physical server is a major concerns for cloud users.. Virtual networks are target for some attacks. We have focused on this distinction, where we consider important to understand these issues. Another core element of cloud computing is multitenancy.

VI. REFERENCES

[1] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., “Scientific Cloud Computing: Early Definition and Experience,” 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 8Paturi V, A. Rakshit, “Cloud Security Issues”, In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009

[2] National Institute of Standards and 25- 830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[3] B. R. Kandukuri, R. Technology, NIST Definition of CloudComputing, Sept 2011.

[4] D. Jamil and H. Zaki, “Security Issues in Cloud Computing and Countermeasures,” International Journal of Engineering Science and Technology, Vol. 3 No. 4, pp.2672-2676, April2011.

http://www.infoworld.com/article/3041078

[5] Rittinghouse JW, Ransome JF: Security in the Cloud. In Cloud Computing. Implementation, Management, and Security, CRC Press; 2009.

[6] Garfinkel T, Rosenblum M: When virtual is harder than real: Security challenges in virtual machine based computing environments. In Proceedings of the 10th conference on Hot Topics in Operating Systems, Santa Fe, NM. volume 10. CA, USA: USENIX Association Berkeley;2005:227-229.

[7] Morsy MA, Grundy J, Muller I: An analysis of the Cloud Computing Security problem. In Proceedings of APSEC 2010 Cloud Workshop. Sydney, Australia: APSEC; 2010.

[8] Farzad Sabahi, "Cloud Computing Security Threats and Responses", 978-1-61284-486- 2, IEEE, 2011, pp: 245 - 249.

[9] Intel IT Center, "Preparing your Virtualized Data Center for the Cloud".