INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp : 54-58

CLOUD STRATEGY AND ARCHITECTURE SERVICES

Mr. Manzoor Ali[1]

[1]CCSU, Meerut, India.

ABSTRACT

Cloud computing is named as such because the information being accessed is found remotely in the cloud or a virtual space. Companies that provide cloud services enable users to store files and applications on remote servers and then access all the data via the Internet. This means the user is not required to be in a specific place to gain access to it, allowing the user to work remotely.

Cloud computing takes all the heavy lifting involved in crunching and processing data away from the device you carry around or sit and work at. It also moves all of that work to huge computer clusters far away in cyberspace. The Internet becomes the cloud, and voilà—your data, work, and applications are available from any device with which you can connect to the Internet, anywhere in the world. Cloud computing is the delivery of computing services over the Internet with less cost and more reliability in getting services. With the increase in need of various technologies which satisfies customer's dynamic resource demands at one place and makes the job easier to work on all platforms for the user from any place with less cost makes the use of cloud important. Security is the main criteria when working on cloud, as the third-party involvement will be there

Keywords: Cloud computing, Architecure, Cloud, Servers, Frontend, Backend, Benfits.

1. INTRODUCTION

CloudComputing?

Cloud computing is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers,databases, networking, and software.

Definition of Cloud Computing

Cloud Computing is rapidly being accepted as a universal access appliance on the Internet. A lot of attention has been given to its concept in deriving standard definitions. But here we consider the standard definition given by the National Institute of Standards and Technology (NIST): "Cloud Computing is model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction", [1].

Cloud Servers?

A cloud server is a compute server that has been virtualized, making its resources accessible to users remotely over a network. Cloud servers are intended to provide the same functions, support the same operating systems (OSes) and applications, and offer similar performance characteristics as traditional physical servers that run in a local data center. Cloud servers are often referred to as virtual servers, virtual private servers or virtual platforms. Cloud servers work by virtualizing physical servers to make them accessible to users from remote locations. Server virtualization is often, but not always, done through the use of a hypervisor. The compute resources of the physical servers are then used to create and power virtual servers, which are also known as cloud servers. These virtual servers can then be accessed by organizations through a working internet connection from any physical location.

Public cloud servers. The most common expression of a cloud server is a virtual machine (VM) -- or compute "instance" -- that a public cloud provider hosts on its own infrastructure and delivers to users across the internet using a web-based interface or console. This model is known as IaaS. Examples of cloud servers include Amazon Elastic Compute Cloud (EC2) instances, Microsoft Azure instances and Google Compute Engine instances.

Private cloud servers. A cloud server may also be a compute instance within an on-premises private cloud. In this case, an enterprise delivers the cloud server to internal users across a local area network (LAN) and, in some cases, also to external users across the internet. The primary difference between a hosted public cloud server and a private cloud server is that the latter exists within an organization's own infrastructure, whereas a public cloud server is owned and operated outside of the organization. Hybrid clouds may include public or private cloud servers. Dedicated cloud servers. In addition to virtual cloud servers, cloud providers can supply physical cloud servers, also known as bare-metal servers, which essentially dedicate a cloud provider's physical server to a user. These dedicated cloud servers -- also called dedicated instances -- are typically used when an organization must deploy a custom virtualization layer or mitigate the performance and security concerns that often accompany a multi- tenant cloud server.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp : 54-58

Benefits of cloud servers. The choice to use a cloud server will depend on the needs of the organization and its specific application and workload requirements. Some potential benefits include.

Ease of use. An administrator can provision a server in a matter of minutes. With a public cloud server, an organization does not need to worry about server installation, maintenance or other tasks that come with owning a physical server.

Globalization. Public cloud servers can globalize workloads. With a traditional centralized data center, admins can still access workloads globally, but network latency and disruptions can reduce performance for geographically distant users. By hosting duplicate instances of a workload in different global regions, organizations can benefit from faster and often more reliable access.

Cost and flexibility. Public cloud servers follow a pay-as-you-go pricing model. Compared to a physical server and its maintenance costs, this can save an organization money, particularly for workloads that only need to run temporarily or are used infrequently.

Cloud servers are often used for temporary workloads, such as software development and testing, as well as for workloads where resources need to be scaled up or down based on demand. However, depending on the amount of use, the long-term and full-time cost of cloud servers can become more expensive than owning the server outright. Furthermore, a full breakdown of cloud computing expenses is important to avoid hidden costs

2. LITERATURE REVIEW

In [10] authors describe Cloud computing has surpassing shifted so far in terms of utilizing the current technologies. The tr end of having cloud services as part of an organization seems to be gaining more importance.

For the reduction of capital expenditures, organizations need to consider utilizing cloud services as an essential part of their foundations. Nevertheless, various challenges are prohibiting the attainment of vast deployment and acceptance levels and the main drawback of the existing cloud service implementations is their inability to provide an accredited high security level. In [11] they first discussed security issues for cloud which include storage security, data security, network security, middleware security and application security.

Main goal is to manage data and securely store that is not controlled by the owner of the data. In particular, they are taking a bottom up approach to security in which they are working on small problems in the cloud that will solve the larger problem of cloud security. We discussed how secure co- processors may be used to enhance security. They implemented the Hadoop finally. Many new technologies emerging at a rapid rate, each with technological advancements and potential of making human's lives easier.

However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. In [12] authors study different architectures which are based on the services they provide. Data is stored on to centralized location called data centers having a large size of data storage. Data as well as processing is somewhere on servers. So, the clients have to trust the provider on the availability as well as data security.

Before moving data into the public cloud, issues of compatibility and security standards must be addressed. A trusted monitor installed at the cloud server that can auditor monitor the operations of the cloud server. In minimizing potential security trust issues as well as adhering to governance issues facing Cloud computing, a prerequisite control measure is to ensure that a concrete Cloud computing ServiceLevel.

3. ARCHITECTURE

Cloud Computing , which is one of the demanding technology of the current time and which is giving a new shape to every organization by providing on demand virtualized services/resources. Starting from small to medium and medium to large, every organization use cloud computing services in storing information and accessing that from anywhere and any time only with the help of internet. In this article we will know more about the internal architecture of cloud computing.

Transparency, scalability, security and intelligent monitoring are some of the most important constraints which every cloud infrastructure should experience. Current research on other important constraints is helping cloud computing system to come up with new features and strategies with a great capability of providing more advanced cloud solutions

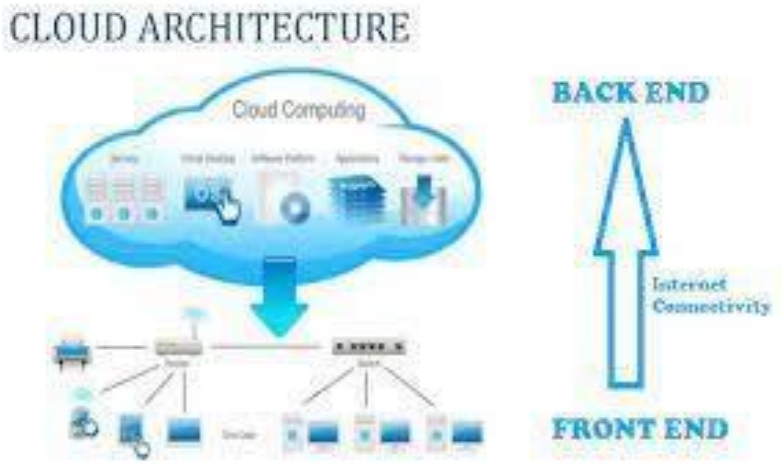
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp : 54-58

e-ISSN : 2583-1062

Impact Factor: 5.725



1. Frontend:

Frontend of the cloud architecture refers to the client side of cloud computing system. Means it contains all the user interfaces and applications which are used by the client to access the cloud computing services/resources. For example use of a web browser to access the cloud plat form.

Client Infrastructure – Client Infrastructure refers to the frontend components. It contains the applications and user interfaces which arerequired to access the cloud platform.

2. Backend:

Backend refers to the cloud itself which is used by the service provider. It contains the resources as well as manages the resources and provides security mechanisms. Along with this it includes huge storage, virtual applications, virtual machines, traffic control mechanisms, deployment models etc.

Cloud Application

Application in backend refers to a software or platform to which client accesses. Means it provides the service in backend as per the clientrequirement.

1. Service –

   Service in backend refers to the major three types of cloud based services like SaaS, PaaS and IaaS. Also manages which type of service the user accesses.

2. Cloud Runtime –

   Runtime cloud in backend refers to provide of execution and runtime platform/environment to the virtual machine.

3. Storage –

   Storage in backend refers to provide flexible and scalable storage service and management of stored data.

4. Infrastructure –

   Cloud Infrastructure in backend refers to hardware and software components of cloud like it includes servers, storage, network devices, virtualization software etc.

5. Management –

   Management in backend refers to management of backend components like application, service, runtime cloud, storage, infrastructure, and other security mechanisms etc.

6. Security –

   Security in backend refers to implementation of different security mechanisms in the backend for secure cloud resources, systems, files, andinfrastructure to end-users.

7. Internet –

   Internet connection acts as the medium or a bridge between frontend and backend and establishes the interaction and communication betweenfrontend and backend.

4. SECURITY CHALLENGES IN THE CLOUD

Data Breaches

- Impact to reputation and trust of customers or partners.
- Loss of intellectual property (IP) to competitors, which may impact products release.

- Regulatory implications that may result in monetary loss.
- Brand impact which may cause a market value decrease due to previously listed reasons.
- Legal and contractual liabilities
- Financial expenses incurred due to incident response and forensics

Misconfiguration and Inadequate Change Control- This is one of the most common challenges of the cloud. In 2017, a misconfigured AWS Simple Storage Service (S3) cloud storage bucket exposed detailed and private data of 123 million American households. The data set belonged to Experian, a credit bureau, which sold the data to an online marketing and data analytics company called Alteryx. It was Alteryx that exposed the file. Such instances can be disastrous.

Lack of Cloud Security Architecture and Strategy- Worldwide, organizations are migrating portions of their IT infrastructure to public clouds. One of the biggest challenges during this transition is the implementation of appropriate security architecture to withstand cyberattacks. Unfortunately, this process is still a mystery for many organizations. Data are exposed to different threats when organizations assume that cloud migration is a "lift-and-shift" endeavor of simply porting their existing IT stack and security controls to a cloud environment. A lack of understanding of the shared security responsibility model is also another contributing factor.

Insufficient Identity, Credential, Access and Key Management- Cloud computing introduces multiple changes to traditional internal system management practices related to identity and access management (IAM). It isn't that these are necessarily new issues. Rather, they are more significant issues when dealing with the cloud because cloud computing profoundly impacts identity, credential and access management. In both public and private cloud settings, CSPs and cloud consumers are required to manage IAM without compromising security.

Account Hijacking- Account hijacking is a threat in which malicious attackers gain access to and abuse accounts that are highly privileged or sensitive. In cloud environments, the accounts with the highest risks are cloud service accounts or subscriptions. Phishing attacks, exploitation of cloud-based systems, or stolen credentials can compromise these accounts.

Insider Threat- The Netwrix 2018 Cloud Security Report indicates that 58 percent of companies attribute security breaches to insiders. Insider negligence is the cause of most security incidents. Employee or contractor negligence was the root cause of 64 percent of the reported insider incidents, whereas 23 percent were related to criminal insiders and 13 percent to credential theft, according to the Ponemon Institute's 2018 Cost of Insider Threats study. Some common scenarios cited include: misconfigured cloud servers, employees storing sensitive company data on their own insecure personal devices and systems, and employees or other insiders falling prey to phishing emails that led to malicious attacks on company assets.

Insecure Interfaces and APIs- Cloud computing providers expose a set of software user interfaces (UIs) and APIs to allow customers to manage and interact with cloud services. The security and availability of general cloud services are dependent on the security of these APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent the security policy. Poorly designed APIs could lead to misuse or—even worse—a data breach. Broken, exposed, or hacked APIs have caused some major data breaches. Organizations must understand the security requirements around designing and presenting these interfaces on the internet.

Weak Control Plane- Moving from the data center to the cloud poses some challenges for creating a sufficient data storage and protection program. The user must now develop new processes for data duplication, migration and storage and—if using multi-cloud—it gets even more complicated. A control plane should be the solution for these problems, as it enables the security and integrity that would complement the data plane that provides stability and runtime of the data. A weak control plane means the person in charge—either a system architect or a DevOps engineer—is not in full control of the data infrastructure's logic, security and verification. In this scenario, controlling stakeholders don't know the security configuration, how data flows and where architectural blind spots and weak points exist. These limitations could result in data corruption, unavailability, or leakage.

Metastructure and Applistructure Failures- Cloud service providers routinely reveal operations and security protections that are necessary to implement and protect their systems successfully. Typically, API calls disclose this information and the protections are incorporated in the metastructure layer for the CSP. The metastructure is considered the CSP/customer line of demarcation—also known as the waterline. Failure possibilities exist at multiple levels in this model. For example, poor API implementation by the CSP offers attackers an opportunity to disrupt cloud customers by interrupting confidentiality, integrity, or availability of the service.

Limited Cloud Usage Visibility- Limited cloud usage visibility occurs when an organization does not possess the ability to visualize and analyze whether cloud service use within the organization is safe or malicious. This concept is broken down into two key challenges. Un-sanctioned app use: This occurs when employees are using cloud applications and resources without the specific permission and support of corporate IT and security. This scenario results in a self-support model called Shadow IT. When insecure cloud services activity does not meet corporate guidelines, this behavior is risky— especially when paired with sensitive corporate data. Gartner predicts that by 2020, one-third of all successful security attacks on companies will come through shadow IT systems and resources.

5. CONCLUSION

Cloud computing is the development trend of IT industry as a new technology which is expected to significantly reduce the cost of existing technologies. In conclusion, cloud computing is recently new technological development that has the potential to have a great impact on the world. It has many benefits that it provides to it users and businesses. For example, some of the benefits that it provides to businesses, is that it reduces operating cost by spending less on maintenance and software upgrades and focus more on the businesses it self. But there are other challenges the cloud computing must overcome. People are very skeptical about whether their data is secure and private. There are no standards or regulations worldwide provided data through cloud computing. Europe has data protection laws but the US, being one of the most technological advance nation, does not have any data protection laws. Users also worry about who can disclose their data and have ownership of their data. But once, there are standards and regulation worldwide, cloud computing will revolutionize the future.

6. REFERENCES

[1] https://cloudsecurityalliance.org/artifacts/top-th...

[2] Peter Mell, “The NIST Definition of Cloud”, Reports on Computer Systems Technology, sept., p.7.,2011

[3] https://www.gartner.com/en/newsroom/press-releases

[4] Ni Zhang Di Liu Yun-Yong Zhang, “Research on cloud computing security”, International Conference on Information Technology and Applications, IEEE,2013

[5] Rabi Prasad Padhy , ManasRanjanPatra , Suresh Chandra Satapathy , “ Cloud Computing: Security Issues and Research Challenges”, IRACST International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No.2, December 2011

[6] AkhilBehl, KanikaBehl, “Security Paradigms for Cloud Computing”, Fourth International Conference on Computational Intelligence, Communication Systems and Networks, IEEE,2012

[7] Detect Website Malware, (2014, Apr. 22), [Online] Available: https://sucuri.net/website-antivirus/malware-scanning-and-detection

[8] AkhilBehl, KanikaBehl, “An analysis of cloud computing security issues”, World Congress on Information and Communications TechnologiesIEEE,2012

[9] HuagloryTianfield, “Security Issues In Cloud Computing”, International Conferenceon Systems, Man, and Cybernetics ,IEEE, OCT 14-17,2012

[10] A. Kundu, C. D. Banerjee, P. Saha, “Introducing New Services in Cloud Computing Environment”, International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152,2010.

[11] MeikoJensen, JorgSehwenk et al., “Technical Security, Issues in cloud Computing”, IEEE International conference on cloud Computing,2009

[12] Shuai Z; Shufen Z; Xuebin C; Xiuzhen H; (2010), “Cloud Computing Research and Development Trend”, 2nd International conference on Future Networks, 2010. ICFN ' 10. pp 23, 22-24 Jan 2010.

[13] Osama Harfoushi, “Data Security issues and challenges in Cloud Computing: A Conceptual Analysis and Review”, Communications and Network, 2014, 6,15-21

[14] P. Radha Krishna Reddy, “The Security Issues of Cloud Computing over Normal & IT Sector”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 3, p. 4, March2012.