IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Special Issue, 4, Feb 2019 E-ISSN: 2347-2693

# Amazon: Cloud Computing Services and Security

**J.P. Karthika[1*], P. Vennila[2]**

[1]Dept. of Information Technology, Rabiammal Ahamed Maideen College for Women, Tiruvarur, Tamilnadu, India
[2]Dept. of Computer Science, Rabiammal Ahamed Maideen College for Women, Tiruvarur, Tamilnadu, India

*Corresponding Author: a_karthi@yahoo.com*

**Available online at: www.ijcseonline.org**

***Abstract*—**Cloud Computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to increase or down their service requirements. Cloud Computing provides the services to the third party provider who owns the infrastructure. It holds the probable to purge the requirements for setting up of high-cost computing infrastructure for IT-based solutions and services that the industry uses. Many industries, banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the possessions such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied. This paper mainly focuses on three cloud service models, frequently referred to as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). This also discusses with example some major cloud service providers in order to show that how cloud computing will make the business world simpler, more proficient and more specialized.

***Keywords*—**Cloud Security Threats, Cloud Models, SaaS, PaaS, IaaS

## I. INTRODUCTION

Cloud computing is a model for enabling 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]. Third-party clouds enable organizations to focus on their core businesses instead of expending resources on computer infrastructure and maintenance.[1]

Advocates note that cloud computing allows companies to avoid or minimize up-front IT infrastructure costs. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and that it enables IT teams to more rapidly adjust resources to meet fluctuating and unpredictable demand.

The following are the essential key characteristics of the cloud computing which make this technology highly attractive form of business in the future.

Figure1 : Cloud Computing Services

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly

 

outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

## II. CLOUD SERVICE MODELS

As such, it is critical that organizations don't apply a broad brush one-size fits all approach to security across all models. Cloud Models can be segmented into Software as a Service (SaaS), Platform as a service (PaaS) and Integration as a Service (IaaS). When an organization is considering Cloud security it should consider both the differences and similarities between these three segments of Cloud Models.

**Infrastructure as a Service**, or IaaS, gives business access to vital web architecture, such as storage space, servers, and connections, without the business need of purchasing and managing this internet infrastructure themselves. Because of the economies of scale and specialization involved, this can be to the benefit of both the business providing the infrastructure and the one using it. In particular, IaaS allows an internet business a way to develop and grow on demand. Both PaaS and SaaS clouds are grounded in IaaS clouds, as the company providing the software as service is also providing the infrastructure to run the software. Choosing to use an IaaS cloud demands a willingness to put up with complexity, but with that complexity comes flexibility. Amazon EC2 and Rackspace Cloud are examples of IaaS.

**Platform as a Service (PaaS)** clouds are created, many times inside IaaS Clouds by specialists to render the scalability and deployment of any application trivial and to help make your expenses scalable and predictable. Some examples of a PaaS system include: Mosso, Google App Engine, and Force.com. The chief benefit of a service like this is that for as little as no money you can initiate your application with no stress more than basic development and maybe a little porting if you are dealing with an existing app. Furthermore, PaaS allows a lot of scalability by design because it is based on cloud computing as defined earlier in the article. If you want a lean operations staff, a PaaS can be very useful if your app will capitulate. The most important negative of using a PaaS Cloud provider is that these services may implement some restrictions or trade-offs that will not work with your product under any circumstances.

**Software as a Service (SaaS)** is relatively mature, and the phrase's use predates that of cloud computing. Cloud applications allow the cloud to be leveraged for software architecture, reducing the burdens of maintenance, support, and operations by having the application run on computers belonging to the vendor. GMail and Salesforce are among examples of SaaS run as clouds, but not all SaaS has to be based in cloud computing.

## III. CLOUD COMPUTING AMAZON WEB SERVICES

Cloud security at AWS is the highest priority. As an AWS customer, you will benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations. An advantage of the AWS cloud is that it allows customers to scale and innovate, while maintaining a secure environment. Customers pay only for the services they use, meaning that you can have the security you need, but without the upfront expenses, and at a lower cost than in an on-premises environment. Amazon was the first major cloud provider, with the 2006 offering of Amazon Simple Storage Service (Amazon S3). The growing cloud market since saw rapid development of Amazon's cloud platform as well as Microsoft's Azure platform and the Google Cloud Platform, and the three vendors continue to jockey for the lead on a variety of cloud fronts today. The vendors are currently engaged in developing cloud-based services around emerging technologies such as machine learning, artificial intelligence (AI) and containerization The AWS technology is implemented at server farms throughout the world, and maintained by the Amazon subsidiary. Fees are based on a combination of usage [1], the hardware/OS/software/networking features chosen by the subscriber, required availability, redundancy, security, and service options.

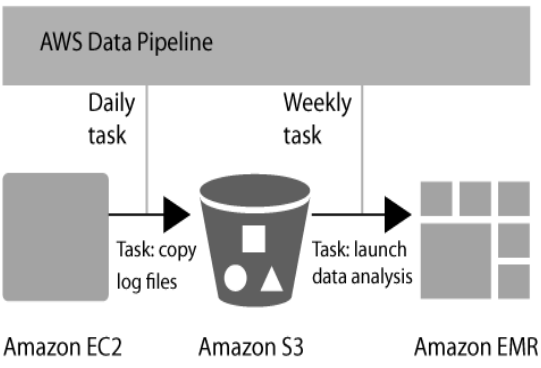


Figure 2 : Amazon Web Services

Subscribers can pay for a single virtual AWS computer, a dedicated physical computer, or clusters of either. As part of the subscription agreement

 

## IV. SECURITY CONTROLS

Cloud security architecture is effective only if the correct defensive implementations are in place. An efficient cloud security architecture should recognize the issues that will arise with security management.[8] The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories:[8]

Deterrent controls : These controls are intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed. (Some consider them a subset of preventive controls.)

Preventive controls : Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

Detective controls : Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue.[8] System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure[2].

Corrective controls : Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.

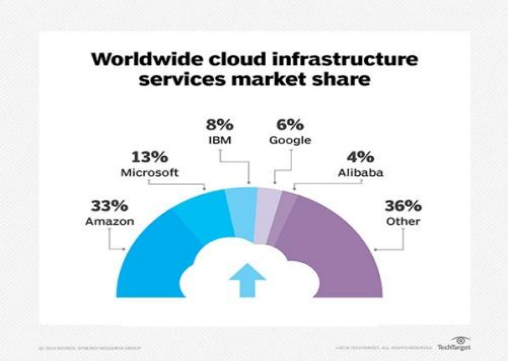


Figure 3: Cloud Infrastructure Services Market Share

## V. DATA SECURITY

A number of security threats are associated with cloud data services: not only traditional security threats, such as network eavesdropping, illegal invasion, and denial of service attacks, but also specific cloud computing threats, such as side channel attacks, virtualization vulnerabilities, and abuse of cloud services. The following security requirements limit the threats.[14]

*1) Confidentiality*

Data confidentiality is the property that data contents are not made available or disclosed to illegal users. Outsourced data is stored in a cloud and out of the owners' direct control. Only authorized users can access the sensitive datawhile others, including CSPs, should not gain anyinformation of the data. Meanwhile, data owners expect to fully utilize cloud data services, e.g., data search, data computation, and data sharing, without the leakage of the data contents to CSPs or other adversaries.

*2) Access controllability*

Access controllability means that a data owner can perform the selective restriction of access to her or his data outsourced to cloud. Legal users can be authorized by the owner to access the data, while others can not access it without permissions. Further, it is desirable to enforce fine-grained access control to the outsourced data, i.e., different users should be granted different access privileges with regard to different data pieces. The access authorization must be controlled only by the owner in untrusted cloud environments.

*3) Integrity*

Data integrity demands maintaining and assuring the accuracy and completeness of data. A data owner always expects that her or his data in a cloud can be stored correctly and trustworthily. It means that the data should not be illegally tampered, improperly modified, deliberately deleted, or maliciously fabricated. If any undesirable operations corrupt or delete the data, the owner should be able to detect the corruption or loss. Further, when a portion of the outsourced data is corrupted or lost, it can still be retrieved by the data users.

## VI. CONCLUSION AND FUTURE SCOPE

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. ... Users also worry about who can disclose their data and have ownership of their data. AWS provides a number of efficient, secure connectivity options to help you get the most out of AWS when integrating your remote networks with

 

Amazon VPC. The options provided in this whitepaper highlight several of the connectivity options and patterns that customers have used to successfully integrate their remote networks or multiple Amazon VPC networks.

## REFERENCES


[1] ("AWS Customer Agreement". *Amazon Web Services, Inc*. Retrieved April 6, 2016.*)*

[2] Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 2010. 179-80. Print.

[3] P. Mell and T. Grance, "Draft nist working definition of cloud computing - v15," 21. Aug 2009, 2009.

[4] https://en.wikipedia.org/wiki/Cloud_computing_security#Data_security

[5] https://searchitchannel.techtarget.com/definition/cloud-service-provider-cloud-provider

[6] (http://status.aws. amazon.com/s3-20080720.html

[7] Platform as Service; http://java.dzone.com/articles/whatplatform-service-paas

[8] https://searchaws.techtarget.com/definition/Amazon-Web-Services


 