

Cloud Computing Architecture & Security: A Survey

Bradley Dodds

Department of Engineering and Computer Science

California State University, Fullerton, CA, U.S.A

ABSTRACT

The use of cloud services has largely increased in recent years, as of 2019, 90% of companies use the cloud. Cloud computing offers businesses a wide variety of benefits such as scalability, security, cost reduction, and access to large amounts of data from any location worldwide. Cloud computing provides an infrastructure for software, platforms, databases, storage and user-based applications. There are three main platforms for cloud computing that include IaaS, PaaS, and SaaS. In this paper, cloud service models will be demonstrated, the infrastructure of cloud security architecture will be explained, and the examination of cloud security risks will be exposed.

KEYWORDS

Cloud computing, cloud security, service models, architecture

1. INTRODUCTION

Cloud computing is the most important component in a company's ability to manage data storage and computing power. Cloud computing delivers access to storage and data over the internet for a low cost. The global cloud computing market is set to reach \$258 billion in 2019 and the majority of companies use a third of their IT budget on cloud-based services.

Cloud services are ideal for companies of any size. One of the most important benefits of using cloud services is scalability. Small companies can easily scale and grow their business due to the flexibility of resources that modern day cloud services provide. Companies can also benefit and use cloud computing services for IoT, analytics, machine learning, software applications and much more. Overall, a company can save operational cost and minimize IT expenses using cloud computing services.

The future of cloud computing and the progression of companies using cloud services is escalating at a fast rate. Since the progression of the cloud is moving at such a rapid pace, many individuals are researching the fundamentals and components of cloud computing. Research include topics such as security of the cloud, cloud service models, benefits, disadvantages, architecture, and much more. This paper will explore some of those fundamental questions.

The fundamental questions that will be summarized and researched in this paper will include the three cloud service models, cloud computing security architecture, and cloud security attacks and

vulnerabilities. The classification scheme used in this study will evaluate trends, identify problems, and compartmentalize leading research on cloud computing.

In this paper, section 2 will present an overview of cloud service models. Section 3 will explain the infrastructure of cloud security architecture. Section 4 will expose cloud security risks and vulnerabilities. Finally, section 5 will provide conclusions and future work.

2. CLOUD SERVICE MODELS

Cloud computing can be broken up into three different service models.

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

Cloud computing can be broken up into three different deployment models.

- Cloud
- Hybrid
- On-Premises

Infrastructure as a Service (IaaS)

Infrastructure as a Service provides the foundation and infrastructure of the cloud. IaaS provide access to networking features such as servers, network devices, hardware, and data storage. This system layer involves the use of virtual machines which can reduce a company's cost in buying physical hardware.

Platform as a Service (PaaS)

Platform as a Service helps a company simplify the process of software development. The platform layer helps reduce the difficult work of software maintenance, capacity planning, operating systems, and hardware. PaaS provides tools and libraries and to have control over application development.

Software as a Service (SaaS)

Software as a Service provides the ease of not managing how the application is managed or maintained but the company determines how the software will be used. Typically, a lightweight application. Allows users to essentially rent the platform application instead of purchasing the software. SaaS has become very popular in modern day business models and brings in a lot of revenue.

Cloud Service Models	Top Cloud Service Providers (2019)
(IaaS) Infrastructure as a Service	Amazon Web Services
(PaaS) Platform as a Service	Microsoft Azure
(SaaS) Software as a Service	Google Cloud
	IBM Cloud
	Oracle Cloud

Businesses today are transitioning more towards the cloud when it comes to application deployment. Deployment models can be broken into three segments, cloud, hybrid, and on-premises.

Cloud deployment represents an application that is completely developed in the cloud and all existing parts of the application run on the cloud.

Hybrid deployment represents an infrastructure that partially uses the cloud or used two different clouds. For instance, some resources may be located in the cloud while other resources may not.

On-premises deployment is also representation of using a private cloud. Typically designed for internal use by a single organization.




3. CLOUD COMPUTING SECURITY ARCHITECTURE

The cloud provides convenience for a modern business to store and manage sensitive data. Many cloud service consumers question the credibility of cloud security and how their data is protected. With many data breaches happening worldwide, this is a valid concern for anyone using cloud services.

Some consumers fail to acknowledge that they are also responsible for implementing their own security measures. Each service model (IaaS, SaaS, PaaS) can have different complexities when it comes to risk exposure. Understanding the differences between the service models and how they are deployed can be key in risk prevention.

The following table represents Cloud computing deployment models presented by Cloud Security Alliance (CSA). Figure taken from [19]

Table 1—Cloud Computing Deployment Models

	Infrastructure Managed By ¹	Infrastructure Owned By ²	Infrastructure Located ³	Accessible and Consumed By ⁴
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community				Trusted
Hybrid	<u>Both Organization & Third Party Provider</u>	<u>Both Organization & Third Party Provider</u>	Both On-Premise & Off-Premise	Trusted & Untrusted

¹ Management includes: governance, operations, security, compliance, etc...

² Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment

³ Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control

⁴ Trusted consumers of service are those who are considered part of an organization's legal/contractual/policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

Cloud Computing Deployment Models

This cloud computing deployment model demonstrates that risk is dependent on different circumstances. These risk factors include the types of resources being managed, who manages the resources, which controls are being selected, and compliance issues. Understanding how a model is deployed can help consumers with risk management.

Cloud Computing Service Models

Each cloud service model is unique and provides different compromises. Understanding the functionality, relationships, and dependencies of each service model is the most important component in understanding cloud computing security.

The following table represents how security gets integrated based off the different service models presented by Cloud Security Alliance (CSA). Figure taken from [22]

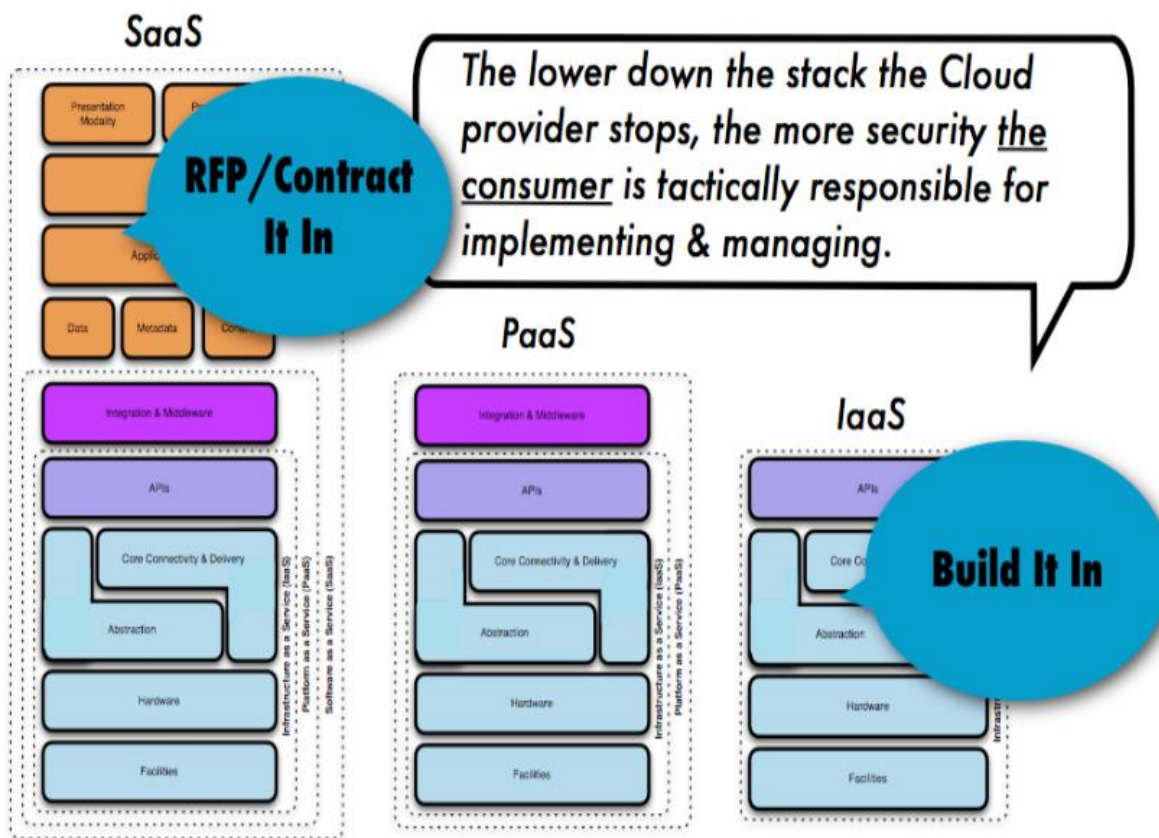


Figure 6—How Security Gets Integrated

4. CLOUD SECURITY ATTACKS

Malicious hackers are always trying find new ways to infiltrate a clouds infrastructure. Being aware of common attacks can help developers and consumers protect themselves against vulnerabilities. A company's worst nightmare is the exposure of sensitive data. Understanding known attacks can help a company ensure security protocols when implementing cloud services such as SaaS, PaaS, or IaaS.

The most common cloud computing attacks involve:

Malware Injection

Vulnerability: SQL Injection, Web Pages

Attack: Manipulating & Stealing Data, Eavesdropping

Malware injection is the injection of malicious code. The malicious code is engineered to present itself as a valid instance in the cloud. Typically, the malicious code represents a service implementation model to a SaaS or PaaS solution. If the malicious instance is undetected and accepted, the attacker can achieve activities such as manipulating data, stealing data, and eavesdropping.

Wrapping Attacks

Vulnerability: XML Signature Element Wrapping, SOAP message header

Attack: Unauthorized Access, Data manipulation, Eavesdropping

Wrapping attacks allow attackers to intrude through the transport layer service. The body of a SOAP message and the signature value is duplicated and sent to the server as a legitimate user. Once the malicious user gains access, they can intrude on the cloud.

Denial of Service

Vulnerability: Server computational Jobs

Attack: Illegitimate processes, Services Starve, Offload to another server, DoS

A DoS attack is when a server is purposely overloaded to deny service to its authentic users. When illegitimate processes are used to disrupt and overload the server it causes the legitimate processes to starve. Resulting in a denial of service.

5. CONCLUSIONS AND FUTURE WORK

Cloud computing plays a vital role in the infrastructure of a modern-day business. The foundation and integrity of a cloud infrastructure is protected by both the consumer and cloud service provider. Understanding service models and how they are deployed can help consumers protect themselves from potential threats by adding additional layers of security. Learning from previous attacks and known vulnerabilities, cloud service developers can protect themselves from malicious events. In future work, we will continue to examine new vulnerabilities and attacks against the cloud.

REFERENCES

- [1] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V3.0," Cloud Computing Alliance,
<https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf>
- [2] McLaughlin, T., 2018. Up and Running Serverless: A Practical Development Workflow for AWS Serverless.
- [3] Ingram, C.B., 2019. *Systems and methods for providing an administrative framework in a cloud architecture*. U.S. Patent Application 10/257,069.
- [4] Vijayakumar, T., 2018. *Practical API Architecture and Development with Azure and AWS: Design and Implementation of APIs for the Cloud*. Apress.
- [5] Varia, J., 2008. Cloud architectures. *White Paper of Amazon, jineshvaria. s3. amazonaws.com/public/cloudarchitectures-varia. pdf*, 16.
- [6] Varia, J. and Mathew, S., 2014. Overview of amazon web services. *Amazon Web Services*, pp.1-22.
- [7] Srinivasan, L. and Treadwell, J., 2005. An overview of service-oriented architecture, web services and grid computing. *HP Software Global Business Unit*, 2, pp.1-13.
- [8] Munir, K. and Palaniappan, S., 2013. Secure cloud architecture. *Advanced Computing*, 4(1), p.9.
- [9] Tripathi, A. and Mishra, A., 2011, September. Cloud computing security considerations. In *2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)* (pp. 1-5). IEEE.
- [10] Zunnurhain, K. and Vrbsky, S., 2010, December. Security attacks and solutions in clouds. In *Proceedings of the 1st international conference on cloud computing* (pp. 145-156).