J. Adv. Res. in Cloud Computing, Virtualization and Web Applications
Volume 3, Issue 1 - 2020, Pg. No. 32-36
Peer Reviewed Journal

Article

Security Review for Cloud Vulnerability: Insecure API Implementation

Kapil Dev Sharma

Assistant Professor, Department of CSE, IET Alwar.

INFO

E-mail Id:
skmkapil@gmail.com

How to cite this article:
Sharma KD. Security Review for Cloud Vulnerability: Insecure API Implementation. *J Adv Res Cloud Comp Virtu Web Appl* 2020; 3(1): 32-36.

Date of Submission: 2020-05-10
Date of Acceptance: 2020-05-23

ABSTRACT

The core encounter of any network computing technique is susceptibility. With the cloud computing environment the services are the key utilization from the concept of virtualization. Cloud networks are typically having threats like account hijacking/session riding, data breach, malicious insiders, and insecure API and system vulnerabilities. These practices may be reduced by using secure architectures and stable services. Creating security groups, multi-factor authentication for privilege management, and data protection by shaping and classifying the type, infrastructure control and detective control. But a large problem with API keys is the inclusion of third-party applications or services for health checkups, automating the system for scalability copying snapshots of database where these API keys may be exposed without our knowledge by adding another attacking space. So, vulnerability must always be described in terms of resistance to a certain type of attack.

Keywords: AWS, IaaS, PaaS, SaaS, Linux,Client-Server Architecture

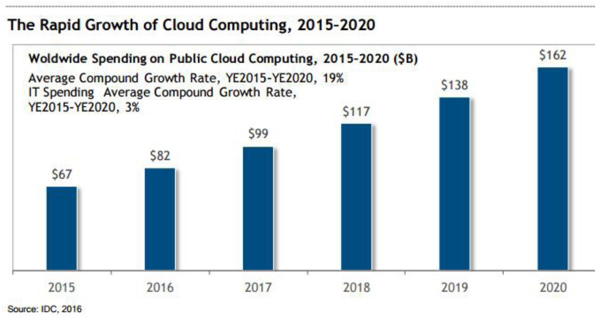
Introduction

Cloud computing is one of the fast growing and adopting virtualization based server technology which offers infrastructure, platform, and software as service.[1] These services are based out of the physical machine and the accessing can reached through instances and containers from various service benefactors like AWS, Google, Azure, IBM's Soft layer, VMW are etc. Instance or in parallel the VM types followed by customized combinations of CPU, memory, storage, and networking capacity and gives a time and cost well-organized planning for IT resources. Popularity reaches due to avoid to invest heavily in data centres and servers, one can pay only when you consume computing resources, and pay only for how much consumed.[2] Each type of cloud service and deployment method has different levels of control, flexibility and management. So, Cloud computing provides a smart way to access servers, storage, databases and a wide set of application services (Proprietary/Open source) over the Internet. As the organizations are affecting in this platform also designates the chances of malpractices. So this paper objective is to make consciousness towards the security threats which can be possible in cloud computing environment and suggest some effective steps to overcome. One of the reasons for insecure API keys in networks is the insecure storage of API keys and improper management or not disposing of the API keys once they're no longer needed. API keys has not reached that level of acceptance just we have to follow their ways to test, scale deploy and manage our cloud infrastructure.[3]

Generic System Architecture

- Cloud computing is the general form for dispersed computing over a network, with the ability to run a machine or use on connected computer infrastructure at the same time.
- Cloud Computing Models

Infrastructure as a Service (IaaS) has the basic building



Source: IDC, 2016

Figure 1.Rapid popularity and growth of cloud computing

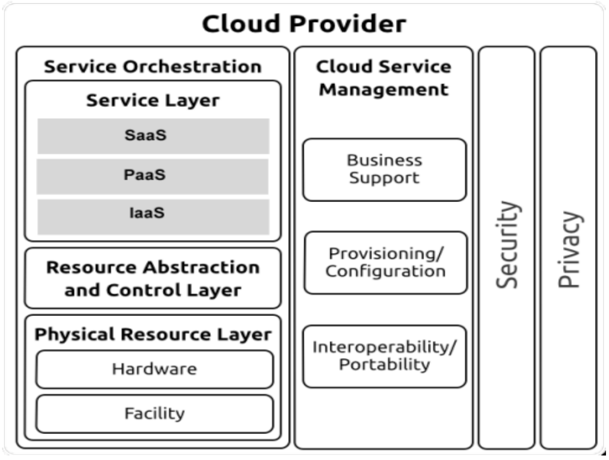


Figure 2.Generic cloud system architecture showing physical resource and virtual services of cloud

blocks for cloud IT resources and afford access to virtual or on devoted hardware (CPU, GPU, RAM, Other computational hardware) and storage drives. IaaS offers the highest level of flexibility and management control over your IT.

Platform as a Service (PaaS) eliminate the need for managing the operating system basically and allows deploying and managing applications.

Software as a Service (SaaS) provides to manage uses, products, and end-user solutions. Consider the e-mail services as an appropriate SaaS service.

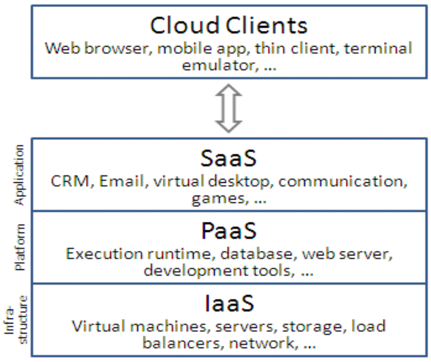

Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...

Figure 3.A layered view of cloud computing system, consisting of three service models (IaaS, PaaS and SaaS)

- Cloud Computing Deployment Models[4]

Cloud

A cloud-based application is completely deployed in the cloud environment and all the layers/ architecture for use run in the cloud.

Hybrid

A hybrid deployment is a mechanism to connect uses and infrastructure between cloud-based resources and existing/ non-cloud resources

On-premises

The deployment of resources on-premises closely related to private cloud using virtualization and resource management.

System Security: Virtualization Vulnerability

Numerous companies are involving in organizing virtualization both in their private and public for enhancing the production and development environment. Usually protecting virtual assets are more difficult than protecting the physical servers. It's also critically important that anyone managing a virtual environment be aware of the evolving threat landscape targeting virtual substructure. This is no dissimilar than the familiar risk management processes done to protect operating systems running on physical servers. Virtualization has become a prime target for malicious activity for the same reason it is popular with IT technocrat.

VMware has identified several major vulnerabilities this year that have required patches for its entire virtualization product line. In May, VMware issued a security advisory to inform customers of five related susceptibilities in its virtualization products. The first two vulnerabilities involved a problem with RPC commands in which a guest could crash the VMX process[5] or execute code on the host. The third vulnerability identified an issue where NFS traffic could potentially overwrite memory, allowing code execution without authentication. The fourth and fifth weaknesses listed in this advisory involved out-of-bounds memory writes with virtual floppy drives and virtual SCSI controllers. These issues were all addressed by installing the appropriate security patch for each VMware product. VMware's advisory included mitigation advice for customers who haven't yet installed the patch, but it may be a little difficult to implement: "Do not allow untrusted users access to your virtual machines. Root- or administrator-level permissions are not required to exploit this issue."[6]

Furthermore, cloud computing systems need to work on security supplies such as confidentiality, authentication, authorization, identity management, integrity, availability, audit, security& health monitoring, incident response, and security policy management. Security in cloud computing spans across all layers of the reference model, ranging from physical security to application security. It's the responsibility of cloud auditor to audit and report security of cloud computing architecture and actors involved. Most of the cloud resource provider have designed and managed their services in alignment with best security practices assurance standards like ISO 9001, ISO 27001, ISO 27018, SOC 1/ISAE 3402, SOC 2, SOC 3, FISMA, DIACAP, and FedRAMP etc.

Cloud Vulnerability: Insecure API Implementation

Cloud computing workers present a set of third party software user interfaces (UIs) or application programming interfaces (APIs) that clienteles use to achieve and interact with cloud services. Provisioning, management, orchestration and monitoring are all achieved with these interfaces.

The obtainability of overall cloud services is dependent on the secure task of these basic APIs. From authentication and admittance control to encryption and movement monitoring, these boundaries must be intended to defend against both accidental and malicious efforts to SLA security policies.[6]

Frequently the governments and third parties can build on these lines to offer various add-on plug-in and value-added services to their customers. Which introduces the complexity of the new covered API; it also intensifications risk, because governments may be obligatory to surrender their credentials to third parties in order to allow their agency. For example, let launch an instance in AWS using AWS CLI or alternate way is using Hashicorp's Terraform and automate the whole procedure by building main.tf and important variables across it. Here AWS is providing the all security to the cloud engine and Terra form is on their end complying all necessary standards, we can move with it. Similarly we have several third party API services which are cost operative and easier to time scale and user complexity but when it comes to their layered architecture, there could be a snapshot or credential threat code.

APIs and UIs are usually the most uncovered part of a system, perhaps the only asset with an IP address available outside the right-hand structural boundary. These assets will be the target of heavy attack, and passable controls defensive them from the Internet are the first line of defense and detection.

Anecdotes and Examples

Moonpig insecure mobile application: Insecure Interface and APIs

Cloudflare/Cloudbleed buffer overrun vulnerability: Shared Technology Vulnerabilities

The IRS Breach and the Importance of Adaptive API Security – "In mid-2015, the US Internal Revenue Service (IRS) exposed over 300,000 records via a vulnerable API." Why Exposed API Keys and Sensitive Data are Growing Cause for Concern – API security involves more than just securing the API itself: it involves protecting API keys, cloud credentials and other sensitive data from public exposure—security measures that are sometimes overlooked by developers.

CCM v3.0.1 Control IDs

AIS-01: Application & Interface Security – Application Security

AIS-04: Application & Interface Security – Data Security/ Integrity

IAM-08: Identity & Access Management – Trusted Sources

IAM-09: Identity & Access Management – User Access Authorization

Discussion

There are 4 layers of cloud application security

Cloud antivirus software involves scanning suspicious files using multiple antivirus engines. Programs or documents are sent to a network cloud where multiple antivirus and behavioral detection programs are working instantaneously in order to improve detection rates.

Secure coding and secure by design means that cloud application is developed in such a way that it is protected against accidental security vulnerabilities. Malicious practices are taken for granted and cloud application is designed in such a way, that when vulnerability is detected it will cause the minimal impact on a system.

Cloud application security is improved on a network level with cryptographic methods and security protocols, such as Secure Sockets Layer (SSL), succeeded by Transport Layer Security (TLS) for web traffic, Pretty Good Privacy (PGP) for email, and IPsec for the network layer security.

Are industrialized on secure operating systems, such as Ubuntu or BSD or Debian.

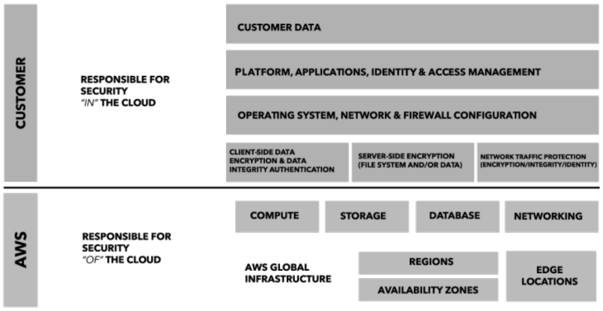

CUSTOMER
RESPONSIBLE FOR SECURITY "IN" THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORK TRAFFIC PROTECTION (ENCRYPTION/INTEGRITY/IDENTITY)
AWS
RESPONSIBLE FOR SECURITY "OF" THE CLOUD
COMPUTE
STORAGE
DATABASE
NETWORKING
AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

Figure 4.AWS Shared responsibility model

Cloud data security is one of the main concerns of any governments, beforehand shifting to the cloud. The data owners can safeguard the data security at its buildings using firewalls, VPN (Virtual Private Network) like most used security options. But as data owner stores their sensitive data to distant servers and user's admission obligatory data from these distant cloud servers, which is not under their control. So storing data outside client premises raises the issue of data security. In this examination paper, procedures followed remember arrangement of the information for the premise of their affectability and significance, trailed by the different cryptography strategies, for example, the AES (a Symmetric Cryptography strategy), SHA-1 (a Hashing method), and ECC (Elliptic bend Cryptography (an Asymmetric Cryptography technique).[7]

Third party tools which are commonly being used with cloud services such as AWS, Azure, Google Cloud etc.

Docker: Container & Image creation

Container: portable package applications

GIT: Source management

Kubernetes: Automating deployment, scaling and management of containerized applications

Chef: configuration management tool

Puppet: configuration management tool

Vagrent: building and maintaining portable virtual software;

Boto3: AWS SDK for python

Ansible: Configuration management tool

Appdynamics: Application Presentation Monitoring & Management

.json-JavaScript Object Notation

.yml- data serialization language for configuration files

Terraform-define a datacenter infrastructure in a high-level configuration language

Gradle: shape engine and automation

Jenkins: Workflow management, Automation testing

JIRA: bug tracking, issue tracking, and project management functions

Gerrit: Code review and verification builds

Sonar: Code analysis and metrics

Jacoco: code coverage

Artifactory: binary artifacts storage and management

With employees, customers, business partners, suppliers and contractors increasingly accessing corporate applications and data with mobile devices from the cloud, protecting the edge of the network is no longer enough. Here are few suggestive measures things to do to help ensure security in the cloud.

Know who's accessing

Individuals within the society who are privileged users, -such as database administrators and personnel with admittance to extremely appreciated intelligent possessions-must obtain a higher level of scrutiny, receive training on securely treatment data, and tougher access control.

Limit data access based on user context

Change the level of access to data in the cloud depending on where the user is and what device they are using.

Take a encryption algorithm-based approach to securing assets used in the cloud

Identify databases with highly sensitive or valuable data and provide extra protection, encryption and monitoring around them.

Extend security to the device

Guarantee that business data is remote from personal data on the mobile device. Install a patch organization agent on the device so that it is always running the latest level of software. Scan mobile uses to check for weaknesses.

Enhance intellect to network defense

The network still requirements to be threatened – never more so than in the cloud. Network defense devices need to have the ability to deliver extra control with analytics and vision into which users are retrieving what content and uses.

Addition a layer of progressive analytics - a security intellect layer-transports all of this security data composed to deliver real-time visibility into the both the Data Centre and the cloud infrastructure.

Conclusion

While most suppliers endeavor to guarantee that security is very much coordinated into their administration models, it is basic for buyers of those administrations to comprehend the security suggestions related with the utilization, the board, arrangement and observing of cloud administrations. Dependence on a frail arrangement of interfaces and APIs opens associations to an assortment of security issues identified with secrecy, uprightness, accessibility and responsibility. Danger displaying applications and frameworks, including information streams and engineering/plan, become significant ordinary pieces of the advancement lifecycle. In addition to security-specific code reviews, rigorous penetration testing becomes a requirement.

References

1. Zhu G, Yin Y, Cai R et al. Detecting Virtualization Specific Vulnerabilities In Cloud Computing Environment. 2017 IEEE 10th *International Conference On Cloud*

Computing: 743-748.

2. Efozia NF, Ariwa E, Asogwa DC et al. A Review Of Threats And Vulnerabilities To Cloud Computing Existence. The Seventh International Conference Of Innovative Computing Technology(INTECH 2017): 197-204
3. Teng Y, Wang X. Research On The Application Of Openstack To Build A New Hetrogeneous Real-Time Virtual Cloud To Reproduce Application Vulnerability And Training Demonstration Architecture, 978-1-5090-6414-4/17/$31.00 , 2017 IEEE pp. 1304-1308
4. Sill A. The Design And Architecture Of Microservices" Ieee Cloud Computing Published By The IEEE Computer Society Issn 2325-6095/2016 Pp.76-80
5. Grobauer B. Tobias Walloschek, And ElmarStöcker "Understanding Cloud Computing Vulnerabilities" Copublished By The IEEE Computer And Reliability Societies, ISSN 1540-7993/2011: 50-57
6. Jon-Michael C. Brook, Field S, Shackleford D. The Treacherous 12 - Top Threats To Cloud Computing+Industry Insights. 2017 Cloud Security Alliance.
7. Goyal V, Kant C. An Effective Hybrid Encryption Algorithm for Ensuring Cloud Data Security" Part of the Advances in Intelligent Systems and Computing book series (AISC, volume 654)Big Data Analytics pp 195-210