International Journal of Research in Social Sciences
Vol. 9 Issue 3, March 2019,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Cloud Security in Cloud Computing

Alok Tuli, AssistantProfessor
AdarshBhartiya College, Pathankot

Abstract

Cloud security or cloud computing security, consists of a set of controls, procedures policies, and technologies that work together to protect cloud-based systems and infrastructure. These security compute are configured to protect the cloud data, support and protect customers' privacy of data and also setting authentication rules for individual users and devices. From documentation access to filtering traffic, cloud security can be configured to the exact needs of the business. These rules can be structure and managed in one place, administration overheads are reduced and IT teams empowered to focus on other areas of the business. The cloud is a collection of servers housed in massive and owned by some of the world's largest corporations. Our data stores on computers we do not have access to. Microsoft, Amazon and Apple have all invested large sums in creating homes for our personal data.

Keywords:*Cloud Security, Cloud Computing,Private Clouds, Hybrid Clouds,Disaster Recovery*

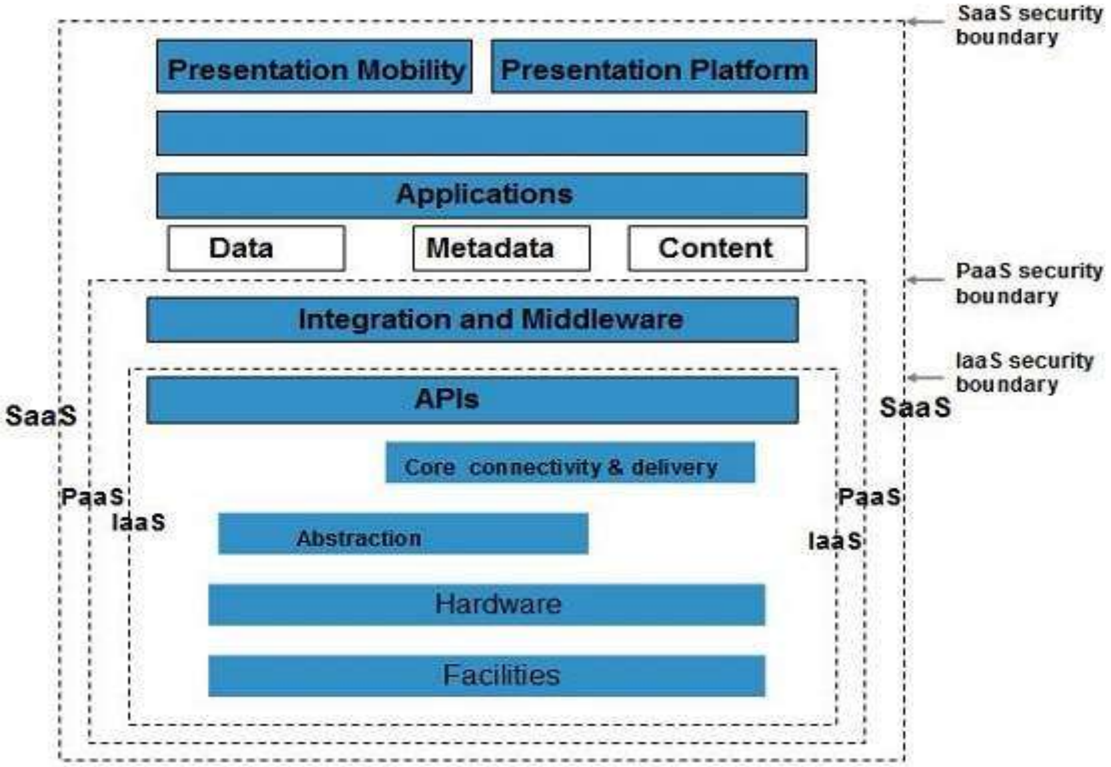
Introduction

Cloud security requires the procedures and technology that secure cloud computing environments against both external and inside cybersecurity threats from out side. Cloud computing means is the delivery of information technology services over the internet and has become a must for businesses and governments seeking to accelerate collaboration and innovation . Cloud security and security management for best practices designed to prevent intruder access are required to keep data and applications in the cloud secure from current & emerging cyberscurity issues. Cloud computing is the delivery of hosted services, including software and storage, over the Internet. The benefits of quick deployment, flexibility, low up-front costs, and scalability, have made cloud computing virtually universal among organizations of all sizes, often as part of a hybrid or Multi-cloud infrastructure .Cloud security refers to the policies, controls, technologies and services that protect cloud data, applications, and infrastructure from threats.

Understanding Security of Cloud

Security Boundaries

A particular service model defines the boundary between the responsibilities of service provider and customer. **Cloud Security Alliance (CSA)** model defines the boundaries between each service model and shows how different functional units relate to each other. The following diagram shows the **CSA stack model:**



Key Points to CSA Model

IaaS is the most fundamental level of service with PaaS and SaaS next two above levels of services.

•Moving upwards, each of the service inherits potentiality and security concerns of the model beneath.

•IaaS provides the architecture, PaaS provides platform development environment and SaaS provides operating environment.

•IaaS has the least small plains the security boundaries at which cloud service provider's responsibilities from end and the customer's responsibilities from begin.

•Any security mechanism below the security boundary must be built into the system and should be maintained by the customer.

Although each service model has safty mechanism, the safty needs also depend upon where these services are located, in private, public, hybrid or community cloud.

The Three Primary Types of Cloud Environments Include

Public Cloud Services

Hosted by 3rd party cloud service providers eg. Amazon Web Services (AWS), Microsoft Azure, Google Cloud and generally accessible through web browsers, so identity management and access control are essential.

Private Clouds

Usually dedicated and accessible to only a individual organization. However, they are still unprotected to access breaches, social engineering, and other exploits.

Hybrid Clouds

Combine aspects of public and private clouds which allowing organizations to wield more control over their data and resources than in a public cloud environment, yet still be able to tap into the scalability and other benefits of the public cloud when needed.

Cloud security controls

Cloud security architecture is most effective only if the correct protective implementations are in place. Anwell organized cloud security architecture should recognize the issues that will arise with security governance. The security governance addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system which reduce the effect of an attack. While there are many types of controls beyond a cloud security architecture, they can usually be found in one of the following categories:

Deterrent controls

These controls are intended to lower attacks on a cloud system. Much like a warning sign on a fence or deterrent controls typically reduce the threat level by informing potential intruders that there will be adverse results for them if they proceed.

Preventive controls

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

Detective controls

Investigator controls are intended to detect and react correctly to any incidents that occur. In the event of an Intruder attack, a detective control will signal the preventative or corrective controls to address the issue. System security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting infrastructure.

Corrective controls

Corrective controls decrease the consequences of an incident, normally by limiting the destruction. They come into effect during an incident. Restoring system reserve in order to rebuild a compromised system is an example of a corrective control.

The Main Cloud Service Models Generally Fall into Three Categories

Infrastructure as a Service (IaaS)

Enables on-demand model for pre-configured virtualized data center computing resources such as network, storage, and operating systems. This can involve automating the creation of virtual machines at scale, so it is critical to consider how virtual machines are provisioned and managed.

Platform as a Service (PaaS)

It Provides tools or other computing infrastructure, enabling organizations to focus on building and running web applications and services. PaaS environments initinally support developers, operations, and DevOps teams. Here, management and configuration of self-service entitlements /privileges is key to controlling risk.

Software as a Service (SaaS)

These are consists of applications hosted by a third party and usually delivered as software services over a web browser that is accessed on the client's side. While the SaaS eliminates the need to deploy and manage applications on end-user devices, potentially any employee can access web services and download content. Thus, proper visibility or access controls are required to monitor types of SaaS applications accessed, usage, and cost.

The Principal Cloud Computing Security Considerations

Lack of Visibility & Shadow IT

Cloud computing makes it easy for aeveryone to subscribe to a SaaS application. Users should Support to strong acceptable use policies for obtaining authorization for, and for subscribing to, new cloud services or creating new instances.

Lack of Control

Leasing a public cloud service means organization does not have ownership of the hardware, applications, software on which the cloud services run. Ensure that you will understand the cloud vendor's approach to these assets.

Transmitting & Receiving Data

Cloud applications often integrate or interface with other services, databases, and applications.These typically achieved through an application programming interface (API). It's to understand the applications and people who have access to API data and to encrypt any sensitive information.

Embedded/Default Credentials & Secrets

Cloud applications which may contain embedded and default credentials. Default recommendations post an increased risk as they may be guessable by attackers. Organizations need to manage these recommendation as they would other types of privileged credentials.

Incompatibilities

IT tools architecture for on-premise environments and one type of cloud are frequently incompatible with other cloud environments. Incompatibilities can translate into visibility and control gaps that uncover organizations to risk from misconfigurations, vulnerabilities and huge dataprivileged access.

Multitenancy

Multitenancy is the backbone for many of cloud benefits of shared resources e.g., lower cost, flexibility, etc but it also introduces concerns about data isolation or data privacy.

Scalability Cuts Both Ways

Automation and rapid scalability are most benefits of cloud computing, but the flip side is that vulnerabilities, mis-configurations.Other security system such as sharing of secrets APIs, privileged credentials, SSH keys, etc can also proliferate at speed and scale. For exp, cloud administrator consoles enable users to swiftly provision, configure, and delete servers at huge scale. However, each of these virtual machines were born with their own set of privileged accounts, which need to be properly onboarded and managed. This can be further compounded in DevOps environments, which by nature are fast charging and highly-automated tend to treat security .

Malware & External Attackers

Attackers can make a living by exploiting cloud unprotected. Rapid detection, and a multilayered security approach firewalls, data encryption, vulnerability management, threat analytics, identity management, etc. will help you to reduce risk, while leaving you better poised to respond to with stand an attack.

Insider Threats – Privileges

Insider threats either through the negligence or malevolence, generally take the longest to detect and resolve, with the potential to be the most harmful. A strong identity / access management framework along with effective privilege management tools are essential to remove these threats and reducing the damage such as by preventing lateral movement and privilege escalation .when they do occur.

9 Cloud Computing Security Best Practices

Strategy & Policy

Holistic cloud security program should account for ownership and accountability (internal or External) of cloud security risks, gaps in protection or compliance, and identify controls needed to mature security and reach the desired end state.

Network Segmentation

In multi-tenant environments, assess what segmentation is in place between your resources and those of other customers, as well as between your own instances. Leverage a zone approach to isolate instances, containers, applications, and full systems from each other when possible.

Identity and Access Management and Privileged Access Management

Leverage robust identity management and verification processes to ensure only authorized users to have access to the cloud environment and applications. Enforce least the privilege to restrict privileged access and to harden cloud resources for instance and only expose resources to the Internet as is necessary, and de-activate unneeded capabilities/features/access). Ensure that privileges are role-based, and that privileged access is audited and recorded via session monitoring.

Discover and Onboard Cloud Instances and Assets

Once cloud instances, services, and assets are made and grouped, bring them under management such as managing and cycling passwords, etc.

Password Control (Privileged and Non-Privileged Passwords)

Never allow the use of shared passwords with some one. Combine passwords with other and authentication systems for sensitive areas. Ensure password management best practices and unique.

Vulnerability Management

Regularly that perform vulnerability, scans and security audits, and patch known vulnerabilities.

Encryption

Ensure thatyour cloud data is encrypted, at rest, and in transit.

Disaster Recovery

Be alert of the data backup and recovery policies and processes for your cloud vendor(s). Do they meet your internal security standards?

Monitoring, Alerting, and Reporting

Implement continual security and user activity are monitoring across all environments . Try to integrate and centralize data from your cloud provider with data from in-house and other vendor solutions,.so you have a holistic picture of what is happening in your data environment.

Conclusion

Aside from the security and compliance issues enumerated above, cloud providers and their customers will conclude terms around liability (stipulating how incidents involving data loss or compromise will be resolved, for example), conceptual property, and end-of-service (when data and applications are ultimately returned to the customer). In addition, there are considerations for acquiring data from the cloud that may be involved in litigation Providers ensure that all critical data such as credit card numbers, for example are masked or encrypted and that only authorized costomers have access to data . Moreover, digital identities must be protected as should any data that the provider collects or produces about customer activity in the cloud. Cloud service providers secure the IT hardware such as servers, routers, cables etc. against unauthorized intruder access, interference, fires, floods etc and ensure that essential supplies are sufficiently robust to minimize the possibility of distoring. This is normally achieved by serving cloud applications from 'world-class' such as professionally specified, designed, constructed, managed, monitored and maintained secure data centers. Various information security systems concerns relating to the IT and other professionals with cloud services are typically handled to pre-, para- and post-employment activities such as security screening potential recruits, security awareness and training programs.

References

1. *Attrapadung, Nuttapong; Herranz, Javier; Laguillaumie, Fabien; Libert, Benoît; de Panafieu, Elie; Ràfols, Carla (2012-03-09).* "Attribute-based encryption schemes with constant-size ciphertexts". *Theoretical Computer Science.* ***422****: 15–38.* doi:10.1016/j.tcs.2011.12.004.
2. *Bethencourt, John;* Sahai, Amit*; Waters, Brent.* "Ciphertext-Policy Attribute-Based Encryption"(PDF). *IEEE Symposium on Security and Privacy 2007. pp. 321–334.*

3. *Bethencourt, John;* Sahai, Amit*; Waters, Brent.* "Ciphertext-Policy Attribute-Based Encryption"(PDF). *IEEE Symposium on Security and Privacy 2007. pp. 321–334.*
4. Chase, Melissa*; Chow, Sherman S. M. "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption". ACM Conference on Computer and Communications Security 2009. pp. 121–130.*
5. *Goyal, Vipul; Pandey, Omkant;* Sahai, Amit*; Waters, Brent. "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data". ACM Conference on Computer and Communications Security 2006. pp. 89–98.*
6. Haghighat, M.; Zonouz, S.; Abdel-Mottaleb, M. (2015). "CloudID: Trustworthy Cloud-based and Cross-Enterprise Biometric Identification". Expert Systems with Applications. **42** (21): 7905–7916. doi:10.1016/j.eswa.2015.06.025.
7. *Jun Tang, Yong Cui (2016).* "Ensuring Security and Privacy Preservation for Cloud Data Services"(PDF). *ACM Computing Surveys.* ***49****: 1–39.* doi*:*10.1145/2906153. 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.
8. *Sahayini, T (2016). "Enhancing the security of modern ICT systems with multimodal biometric cryptosystem and continuous user authentication". International Journal of Information and Computer Security.* ***8*** *(1): 55.* doi*:*10.1504/IJICS.2016.075310.
9. *Srinivasan, Madhan (2012). "State-of-the-art cloud computing security taxonomies". 'State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment. ACM ICACCI'. p. 470.* doi*:*10.1145/2345396.2345474. ISBN 9781450311960.
10. *Mowbray, Miranda (2009).* "The Fog over the Grimpen Mire: Cloud Computing and the Law". *SCRIPTed.* ***6*** *(1): 129.* doi*:*10.2966/scrip.060109.132.
11. *Ottenheimer, Davi (2012). Securing the Virtual Environment: How to Defend the Enterprise Against Attack. Wiley.* ISBN 9781118155486.
12. *Winkler, Vic (2011).* Securing the Cloud: Cloud Computer Security Techniques and Tactics. *Waltham, MA USA: Elsevier. p. 59.* ISBN 978-1-59749-592-9
13. *Wang, Qian; He, Meiqi; Du, Minxin; Chow, Sherman S. M.; Lai, Russell W. F.; Zou, Qin Zou (2018). "Searchable Encryption over Feature-Rich Data". IEEE Transactions on Dependable and Secure Computing.* ***15*** *(3): 496–510.*