COULD SECURITY MECHANISMS

Miss. Sakshi Ram Singh
(Student, MSc IT 1)
Institute of Distance and Open Learning
University of Mumbai
Mulund College of Commerce, Mumbai

ABSTRACT: Cloud security is also called cloud computing security. It is the set of policies, technologies, applications, and control utilized for virtual infrastructure which includes hardware, software, and application. The field is closely related to database security, web security, network security, etc. In other words, cloud security is very close to computer security, IT security, or information security. Day by day the IT infrastructure becomes a common need of every individual and organization so the security aspect is an important concern in this regard. Cloud computing security is controlled by different mechanisms such as deterrent control, preventive control, detective control, and collective control. Cloud Vulnerability and Penetrating Testing are very much important for secure and healthy cloud security practices. Cloud Computing is an important name in the IT and Computing domain and this is rising in different organizations and institutions. In this paper different areas of Cloud Computing have been described. There are different models and architectures for cloud computing security and different rules, regulation, and framework. This paper is conceptual in nature and talks about various areas of security in the basic sense. The paper also talks about Security affairs related to the Cloud.

Key Words: Cloud security, Cloud security tools, Encryption**,** Single sign-on (SSO**),** Public Key Infrastructure,

Introduction: Cloud management mechanisms are measures to be taken to ensure that there are security mechanisms of cloud solutions in place to deal with security attacks and threats. Cloud management and the evolution of the cloud can help to facilitate the controls, Management and the evolution of cloud technology and IT resource that form part of the Cloud platform and solution. As cloud-based IT resources must be configured, set up, Maintained, and monitored, some systems and mechanisms should be in place to

Managed these tasks. The mechanisms of how these systems are managed are discussed are they typically provide Integrated APIs that can offer individual products, and custom applications, which can be combined into various products suites or multi-function applications.

What is Cloud Security?

Cloud security is a set of control-based security measures and technology protection, designed to protect online stored resources from leakage, theft, and data loss. Protection includes data from cloud infrastructure, applications, and threats. Security applications use software the same as SaaS (Software as a Service) model.

Why cloud security is important?

As enterprise cloud adoption grows, business-critical applications and data migrate to trusted third-party cloud service providers (CSPs). Most major CSPs offer standard cyber security tools with monitoring and alerting functions as part of their service offerings, but in-house information technology (IT) security staff may find these tools do not provide enough coverage, meaning there are cyber security gaps between what is offered in the CSP's tools and what the enterprise requires. This increases the risk of data theft and loss.

How cloud security works

Cloud computing operates in three main environments

1. **Public cloud services** are hosted by CSPs. These include software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).
2. **Private clouds** are hosted by or for a single organization.
3. **Hybrid clouds** include a mix of public and private clouds.

Cloud security tools:

Many of the same tools used in on-premises environments should be used in the cloud, although cloud-specific versions of them may exist. These tools and mechanisms include encryption, IAM and single sign-on (SSO), data loss prevention (DLP), intrusion prevention and detection systems (IPSes/IDSes), and public key infrastructure (PKI).

1. Encryption:

Encryption in cryptography is a process by which plain text or a piece of information is converted into cipher text or text which can only be decoded by the receiver for whom the information was intended. The algorithm that is used for the process of encryption is known as cipher.

It helps in protecting consumer information, emails, and other sensitive data from unauthorized access to it as well as secures communication networks. Presently there are many options to choose from and find out the most secure algorithm which meets our requirements. Four such encryption algorithms are highly secured and unbreakable.

2. Single sign-on (SSO**):**

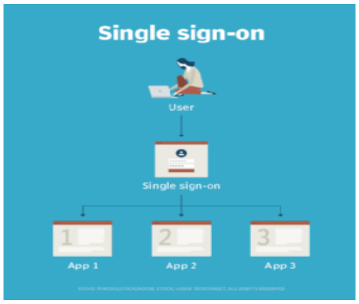
Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials -- for example, a username and password -- to access multiple applications. SSO can be used by enterprises, small and midsize organizations, and individuals to ease the management of multiple credentials.

A. Types of SSO configurations

a) SSO security risk

b) Social SSO

c) Enterprise SSO

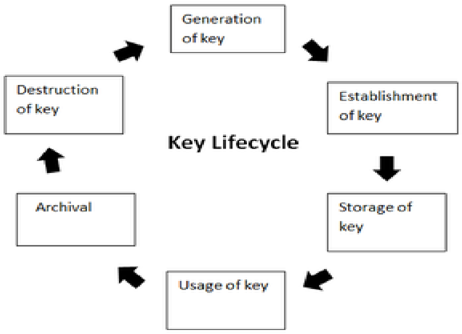

Single sign-on
User
Single sign-on
1
2
3
App 1
App 2
App 3
ICONS: PURESOLUTION/ADOBE STOCK; ©2019 TECHTARGET. ALL RIGHTS RESERVED

3. Public Key Infrastructure:

Public key infrastructure or PKI is the governing body behind issuing digital certificates. It helps to protect confidential data and gives unique identities to users and systems. Thus, it ensures security in communications.

The public key infrastructure uses a pair of keys: the public key and the private key to achieve security. The public keys are prone to attacks and thus an intact infrastructure is needed to maintain them.

Public key infrastructure affirms the usage of a public key.
PKI identifies a public key along with its purpose.



It usually consists of the following components:

- A digital certificate also called a public key certificate
- Private Key tokens
- Registration authority
- Certification authority
- CMS or Certification management system

How to secure data in the cloud

The steps required to secure data in the cloud vary. Factors, including the type and sensitivity of the data to be protected, cloud architecture, accessibility of built-in and third-party tools, and number and types of users authorized to access the data must be considered.

Some general best practices to secure business data in the cloud include the following:

- Encrypt data at rest, in use, and motion.
- Use two-factor authentication (2FA) or multifactor authentication (MFA) to verify user identity before granting access.
- Adopt cloud-edge security protections, including firewalls, IPSes, and antimalware.
- Isolate cloud data backups to prevent ransomware threats.
- Ensure data location visibility and control to identify where data resides and to implement restrictions on whether data can be copied to other locations inside or outside the cloud.
- Log and monitor all aspects of data access, additions, and changes.

Top cloud security challenges

Many of the traditional cyber security challenges also exist in the cloud. These can include the following:

- insider threats
- data loss
- data breaches
- I AM
- key management
- access control
- phishing
- malware
- shadow IT
- distributed denial-of-service (DDoS) attacks
- insecure application programming interfaces (APIs)

As for cloud security challenges specifically, administrators have to deal with issues that include the following:

- cloud account hijacking;
- lack of cloud visibility and control;
- working with cloud security tools that in-house administrators may be unfamiliar with;
- tracking and monitoring where data is located both in transit and at rest;
- misconfigurations;
- weak cloud control plane;
- challenges understanding the shared responsibility model;
- nefarious use of cloud services;

- multi-tenancy concerns;
- incompatibilities with on-premises environments;
- cloud compliance; and
- cloud governance.

Conclusion:

Now as we all know cloud technology growing very fast and became so popular today so In this case, everyone is very curious about their security and data over the internet. So cloud security uses so many mechanisms of network security to make the cloud more Secure and robustness. Various methods available to the easiest method like remote management, billing Management and amp; resource management etc. available to manage your The cloud is more difficult to manage in recent times. Hashing and public Key infrastructure provides strong security enhancement to the cloud Services. As we know cloud services available as private, public, and hybrid, So in this case security is very important to maintain the privacy of the user and Services provider.

References:

https://www.javatpoint.com/what-is-cloud-security
https://patterns.aricture.com/cloud-computing-patterns/mechanisms/remote_administration_system
https://www.deloitte.com/global/en/services/risk-advisory/content/future-of-cyber.html