Cloud Security

> Name: TRY
>
> ID:
>
> Major: Computer science and technology

> Time: 2020/12/23

In the final project, I choose to conduct my mini-research on the topic of "Cloud Security".

Abstract

Cloud Security involves the procedures and technology that secure cloud computing environments against both external and internal cybersecurity threats. **Cloud computing**, which is the delivery of information technology services over the internet, has become a must for businesses and governments seeking to accelerate innovation and collaboration. Cloud security and security management best practices designed to prevent unauthorized access are required to keep data, applications and infrastructure in the cloud secure from current and emerging cybersecurity threats.

Keywords

Cloud Security; Cloud computing; Cybersecurity threat; Cloud Security Algorithm

1. Cloud computing categories

Different cloud security methods should be based on different categories of cloud computing. There are four main categories of cloud computing:

- **Public cloud services, operated by a public cloud provider** : These include software-as-a-service (SAAS), infrastructure-as-a-service (IAAS), and platform-as-a-service (PAAS).
- **Private cloud services, operated by a private cloud provider** : These services provide a computing environment dedicated to one customer, operated by a third party.
- **Private cloud services, operated by internal staff** : These services are an evolution of the traditional data center, where internal staff operates a virtual environment they control.
- **Hybrid cloud services** : Private and public cloud computing configurations can be combined, hosting workloads and data based on optimizing factors such as cost, security, operations and access. Operation will involve internal staff, and optionally the public cloud provider.

The following is a diagram showing common control plane across cloud models:

2. Significance of cloud security

2.1 On-site data security V.S. cloud data security

Cloud security is essential for the many users who are concerned about the safety of the data they store in the cloud. They believe their data is safer on their own local servers where they feel they have more control over the data. However, data stored in the cloud may be more secure because cloud service providers have superior security measures, and their employees are security experts. On-premise data could be more vulnerable to security breaches, depending on the type of attack. Social engineering and malware can make any data storage system vulnerable, but on-site data may be more vulnerable since its guardians are less experienced in detecting security threats.

2.2 Benefits of cloud security

For businesses making the transition to the cloud, robust cloud security is imperative. Security threats are constantly evolving and becoming more sophisticated, and cloud computing is no less at risk than an on-premise environment. For this reason, it is essential to work with a cloud provider that offers best-in-class security that has been customized for your infrastructure.

Cloud security offers various **benefits**, including:

- **Centralized security** : Just as cloud computing centralizes applications and data, cloud security centralizes protection. Cloud-based business networks consist of numerous devices and endpoints that can be difficult to manage when dealing with shadow IT or BYOD. Managing these entities centrally enhances traffic analysis and web filtering, streamlines the monitoring of network events and results in fewer software and policy updates. Disaster recovery plans can also be implemented and actioned easily when they are managed in one place.
- **Reduced costs** : One of the benefits of utilizing cloud storage and security is that it eliminates the need to invest in dedicated hardware. Not only does this reduce capital expenditure, but it also reduces administrative overheads. Where once IT teams were firefighting security issues reactively, cloud security delivers proactive security features that offer protection 24/7 with little or no human intervention.
- **Reduced Administration** : When you choose a reputable cloud services provider or cloud security platform, you can stop setting the manual security configurations and almost constant security updates. These tasks can have a massive drain on resources, but when

you move them to the cloud, all security administration happens in one place and is fully managed on your behalf.
- **Reliability** : Cloud computing services offer the ultimate in dependability. With the right cloud security measures in place, users can safely access data and applications within the cloud no matter where they are or what device they are using.

All cloud models are susceptible to threats. IT departments are naturally cautious about moving mission-critical systems to the cloud and it is essential the right security provisions are in place, whether you are running a native cloud, hybrid or on-premise environment. Cloud security offers all the functionality of traditional IT security, and allows businesses to harness the many advantages of cloud computing while remaining secure and also ensure that data privacy and compliance requirements are met.

3. Segementation cloud security responsibilities

3.1 Cloud security: a shared responsibility

Cloud security is a responsibility that is **shared between the cloud provider and the customer**. Most cloud providers attempt to create a secure cloud for customers. Their business model hinges on preventing breaches and maintaining public and customer trust. Cloud providers can attempt to avoid cloud security issues with the service they provide, but can't control how customers use the service, what data they add to it, and who has access. Customers can weaken cybersecurity in cloud with their configuration, sensitive data, and access policies.

3.2 Categories of responsibilities

There are basically three categories of responsibilities in the Shared Responsibility Model: responsibilities that are *always* the provider's, responsibilities that are *always* the customer's, and responsibilities that *vary depending on the service model*: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS), such as cloud email.

The security responsibilities that are *always* the provider's are related to the safeguarding of the infrastructure itself, as well as access to, patching, and configuration of the physical hosts and the physical network on which the compute instances run and the storage and other resources reside.

The security responsibilities that are *always* the customer's include managing users and their access privileges (identity and access management), the safeguarding of cloud accounts from unauthorized access, the encryption and protection of cloud-based data assets, and managing its security posture.

4. Cloud security challenges

Because the public cloud does not have clear perimeters, it presents a fundamentally different security reality. This becomes even more challenging when adopting modern cloud approaches such as automated Continuous Integration and Continuous Deployment (CI/CD) methods, distributed serverless architectures, and ephemeral assets like Functions as a Service and containers.

Some of the advanced cloud-native security challenges and the multiple layers of risk faced by today's cloud-oriented organizations include:

- **Increased Attack Surface** : The public cloud environment has become a large and highly attractive attack surface for hackers who exploit poorly secured cloud ingress ports in order to access and disrupt workloads and data in the cloud. Malware, Zero-Day, Account Takeover and many other malicious threats have become a day-to-day reality.
- **Lack of Visibility and Tracking** : In the IaaS model, the cloud providers have full control over the infrastructure layer and do not expose it to their customers. The lack of visibility and control is further extended in the PaaS and SaaS cloud models. Cloud customers often cannot effectively identify and quantify their cloud assets or visualize their cloud environmets.
- **Control over cloud data** : In a third-party cloud service provider's environment, IT teams have less access to data than when they controlled servers and applications on their own premises. Cloud customers are given limited control by default, and access to underlying physical infrastructure is unavailable. Besides, cloud assets are provisioned and decommissioned dynamically—at scale and at velocity. Traditional security tools are simply incapable of enforcing protection policies in such a flexible and dynamic environment with its ever-changing and ephemeral workloads.
- **Access to cloud data and applications** : Users may access cloud applications and data over the internet, making access controls based on the traditional data center network perimeter no longer effective. User access can be from any location or device, including bring-your-own-device (BYOD) technology. In addition, privileged access by cloud provider personnel could bypass your own security controls.
- **Compliance** : Use of cloud computing services adds another dimension to regulatory and internal compliance. Your cloud environment may need to adhere to regulatory requirements such as HIPAA, PCI and Sarbanes-Oxley, as well as requirements from internal teams, partners and customers. Cloud provider infrastructure, as well as interfaces between in-house systems and the cloud are also included in compliance and risk management processes.
- **Complex Environments** : Managing security in a consistent way in the hybrid and multicloud environments favored by enterprises these days requires methods and tools that work seamlessly across public cloud providers, private cloud providers, and on-premise deployments—including branch office edge protection for geographically distributed organizations.
- **Cloud-native breaches** : Data breaches in the cloud are unlike on-premises breaches, in that data theft often occurs using native functions of the cloud. A Cloud-native breach is a series of actions by an adversarial actor in which they "land" their attack by exploiting errors or vulnerabilities in a cloud deployment without using malware, "expand" their access through weakly configured or protected interfaces to locate valuable data, and "exfiltrate" that data to their own storage location.
- **Misconfiguration** : Cloud-native breaches often fall to a cloud customer's responsibility for security, which includes the configuration of the cloud service. Research shows that just 26% of companies can currently audit their IaaS environments for configuration errors. Misconfiguration of IaaS often acts as the front door to a Cloud-native breach, allowing the attacker to successfully land and then move on to expand and exfiltrate data. Research also shows 99% of misconfigurations go unnoticed in IaaS by cloud customers. Here's an excerpt from this study showing this level of misconfiguration disconnect:
- **Disaster recovery** : Cybersecurity planning is needed to protect the effects of significant negative breaches. A disaster recovery plan includes policies, procedures, and tools designed to enable the recovery of data and allow an organization to continue operations and business.

- **Insider threats** : A rogue employee is capable of using cloud services to expose an organization to a cybersecurity breach. A recent McAfee Cloud Adoption and Risk Report revealed irregular activity indicative of insider threat in 85% of organizations.

5. Cloud security solution

Organizations seeking cloud security solutions should consider the following criteria to solve the primary cloud security challenges of visibility and control over cloud data.

- **Visibility into cloud data** : A complete view of cloud data requires direct access to the cloud service. Cloud security solutions accomplish this through an application programming interface (API) connection to the cloud service. With an API connection it is possible to view:
    - What data is stored in the cloud.
    - Who is using cloud data.
    - The roles of users with access to cloud data.
    - Who cloud users are sharing data with.
    - Where cloud data is located.
    - Where cloud data is being accessed and downloaded from, including from which device.
- **Control over cloud data** : Once you have visibility into cloud data, apply the controls that best suit your organization. These controls include:
    - **Data classification** : Classify data on multiple levels, such as sensitive, regulated, or public, as it is created in the cloud. Once classified, data can be stopped from entering or leaving the cloud service.
    - **Data Loss Prevention (DLP)** : Implement a cloud DLP solution to protect data from unauthorized access and automatically disable access and transport of data when suspicious activity is detected.
    - **Collaboration controls** : Manage controls within the cloud service, such as downgrading file and folder permissions for specified users to editor or viewer, removing permissions, and revoking shared links.
    - **Encryption** : Cloud data encryption can be used to prevent unauthorized access to data, even if that data is exfiltrated or stolen.
- **Access to cloud data and applications** : As with in-house security, access control is a vital component of cloud security. Typical controls include:
    - **User access control** : Implement system and application access controls that ensure only authorized users access cloud data and applications. A Cloud Access Security Broker(CASB) can be used to enforce access controls.
    - **Device access control** : Block access when a personal, unauthorized device tries to access cloud data.
    - **Privileged access** : Identify all possible forms of access that privileged accounts may have to your data and applications, and put in place controls to mitigate exposure.
    - **Malicious behavior identification** : Detect compromised accounts and insider threats with user behavior analytics (UBA) so that malicious data exfiltration does not occur.
    - **Malware prevention** : Prevent malware from entering cloud services using techniques such as file-scanning, application whitelisting, machine learning-based malware detection, and network traffic analysis.
- **Compliance** : Existing compliance requirements and practices should be augmented to include data and applications residing in the cloud.

    - **Compliance Assessments** : Review and update compliance assessments for PCI, HIPAA, Sarbanes-Oxley and other application regulatory requirements.
    - **Risk assessment** : Review and update risk assessments to include cloud services. Identify and address risk factors introduced by cloud environments and providers. Risk databases for cloud providers are available to expedite the assessment process.
- **Threat intelligence** : detects and remediates known and unknown threats in real-time
    - **Log data**: Third-party cloud security vendors add context to the large and diverse streams of cloud-native logs by intelligently cross-referencing aggregated log data with internal data such as asset and configuration management systems, vulnerability scanners and external data such as public threat intelligence feeds, geolocation databases, etc.
    - **Real-time alerts** : They also provide tools that help visualize and query the threat landscape and promote quicker incident response times. AI-based anomaly detection algorithms are applied to catch unknown threats, which then undergo forensics analysis to determine their risk profile. Real-time alerts on intrusions and policy violations shorten times to remediation, sometimes even triggering auto-remediation workflows.

6. Cloud security algorithms

To provide security to cloud many algorithms are designed. Some popular and classical algorithms are : RSA, Message Digest Algorithm (MDA) , Data Encryption Standard(DES), Advance Encryption Algorithm (AES), Triple-DES(TDES), Blowfish Algorithm, IDEA, Homomorphic Encryption, and etc.

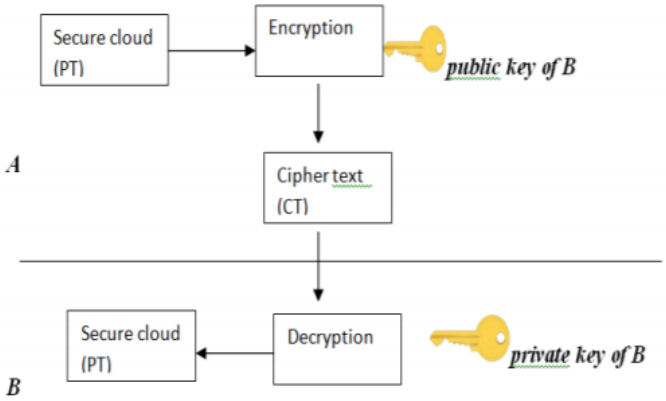
And the following are introductions to RSA and MDA.

6.1 RSA

RSA Algorithm named after its inventers (Rivest, Shamir, and Adelman) is best suited for data traveling to/from Web and Cloud based environments. In working with Cloud Computing, the end user data is first encrypted and then stored on the Cloud. When the data is required, the end user simply needs to place a request to the Cloud Service provider for accessing the data. For this the Cloud service provider first authenticates the user to be the authentic owner and then delivers the data to the requester using RSA Asymmetric Algorithm. This algorithm has support from .NET Security Framework as well.

Third-Party can detect Cloud service provider misbehavior with a certain probability by asking proof for a constant amount of blocks that are independent of the total number of file blocks. Every message block is mapped to an integer value. RSA algorithm consists of Public Key and Private Key. Public Key is known to all cloud users, whereas Private-Key is known only to the user who originally owns the data. Encryption is performed by the Cloud service provider and decryption is performed by the Cloud user/cloud customer. Once the data is encrypted with the Public Key, it can be decrypted with the corresponding Private Key.

RSA algorithm involves three **steps**: 1. Key Generation; 2. Encryption; 3. Decryption .



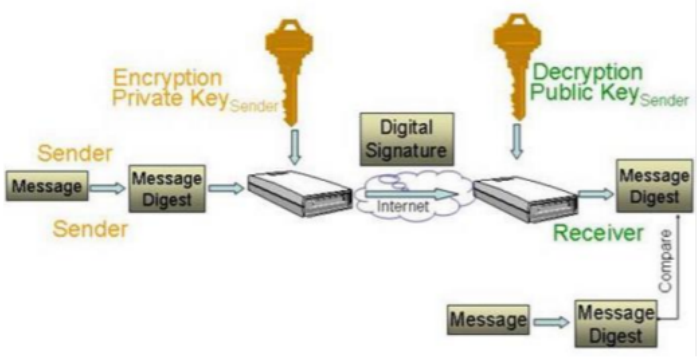
- **Key Generation**: Key is generated by the cloud service provider and the user.
    1. Choose two distinct prime numbers x and y. For security purposes, the integers x and y should be chosen at random and should be of same bit length.
    2. Compute $n = x * y$.
    3. Compute Euler's totient function, $\phi(n) = (x-1) * (y-1)$
    4. Chose an integer PU, such that $1 < PU < \phi(n)$ and greatest common divisor of PU , $\phi(n)$ is 1. Now PU is released as Public-Key exponent.
    5. Now determine PR as follows: $PR = PU - 1(mod\ \phi(n))$ i.e., PR is multiplicate inverse of $PU\ mod\ \phi(n)$.
    6. PR is kept as Private-Key component, so that $PR * PU = 1\ mod\ \phi(n)$.
    7. The Public-Key consists of modulus n and the public exponent PU i.e, (PU, n).
    8. The Private-Key is a combination of modulus n and the private exponent PR, which must be kept secret i.e, (PR, n).
- **Encryption**: The process of converting original plain text to cipher text is called as encryption.
    1. Cloud service provider should transmit the Public Key (n, PU) to the user who wants to store the data with him or her.
    2. User data is now mapped to an integer using an agreed upon reversible protocol, named as padding scheme.
    3. Data is encrypted using the calculation $CT = PT * PU\ (mod\ n)$.
    4. This cipher text is now stored in the Cloud storage.
- **Decryption**: The process of converting the cipher text to the original plain text is known as decryption. Steps:
    1. The cloud user requests the CSP for the data.
    2. CSP verify's the authenticity of the user and gives the encrypted data (CT).
    3. The Cloud user then decrypts the data by computing, $PT = CT * PR(mod\ n)$.
    4. Once PT is obtained, the user can get back the original data by reversing the padding scheme.

6.2 Message Digest Algorithm (MDA)

Message Digest Algorithm (MDA) uses public key encryption, symmetric encryption and standard hashing algorithm in the registration process, authentication process and generating the message digests respectively. As MDA does not have any specification for algorithms, any standard combinations of encryption algorithms and hashing algorithms could be used in the operations of MDA.

Message digest function, also known as hash function is used to generate Digital Signature of the information. The digital signature produced by the hash function is known as message digest. MD5 algorithm is used to implement integrity of the message and it produces message digest of size 128 bits. There are mathematical functions that process data to produce different message digest for each different message.

The algorithm contains the following **steps**: 1. Appending the padding bits; 2. Appending the length; 3. Initializing a MD buffer; 4. Processing message in 512 bit blocks; 5. Generating output



The algorithm consists of **5 functions**:

- **Key Generation**:
  1. Randomly generate two large prime numbers: a and b.
  2. Compute $n = a * b$
  3. Compute the totient: $\Phi\,(n) = (a-1) * (b-1)$
  4. Choose an integer 'c' such that $1 < c < \phi(n)$ and $gcd(c, \phi(n)) = 1$
  5. Compute d, such that $d * c = 1\ mod\ \phi(n)$
  6. The public key is (n, c) and the private key is (n, d).
- **Digital Signing:**
  1. Message digest of the document to be send is generated.
  2. The digest is represented as an integer msg.
  3. Digital Signature DS is generated using the private key(n, d), $DS = msg * d\ mod\ n$. Sender sends this signature DS to the recipient.
- **Encryption**:
  1. Sender exemplifies the plain text message as a positive integer value msg.
  2. It converts the message into encrypted form using the receiver's public key (c, n).
  3. $CT = msg * c\ mod\ n$.
  4. Sender sends this encrypted message to the recipient B.
- **Decryption:** Recipient B does the following operation:
  1. Using his private key (n, d), it converts the cipher text to plain text 'msg'. $msg = CT * d\ mod\ n$.
- **Signature Verification**: Receiver B does the followings to verify the signature:
  1. An integer V is generated using the senders public key (n, c) and signature DS.
  2. $V = DS * c\ mod\ n$.
  3. It extracts the message digest $M1$, from the integer V using the same MD5 algorithm.
  4. It then computes the message digest $M2$ from the signature DS.
  5. If both the message digests are identical i.e. value ($M1$)= value($M2$), then signature is valid.