**An Overview of Cloud Cryptography**

Cloud cryptography is a set of techniques used to secure data stored and processed in cloud computing environments. It provides data privacy, data integrity, and data confidentiality by using encryption and secure key management systems. Common methods used in cloud cryptography include:

1. Symmetric encryption: encrypts and decrypts data using the same key.
2. Asymmetric encryption: uses two different keys, a public key for encryption and a private key for decryption.
3. Hash functions: create a unique digest of a message to ensure its integrity.
4. Key management: securely stores and manages encryption keys to ensure the security of encrypted data.

The use of cryptography in the cloud is essential for protecting sensitive information and ensuring compliance with regulations such as GDPR and HIPAA.

**Cloud Cryptography** is encryption that safeguards data stored within the cloud. Several measures are being placed within cloud cryptography which adds a strong layer of protection to secure data to avoid being breached, hacked or affected by malware. Any data hosted by cloud providers are secured with encryption, permitting users to access shared cloud services securely and conveniently. Cloud Cryptography secures sensitive data without delaying the delivery of information.

**How does cryptography in the cloud work?**

Cloud cryptography is based on encryption, in which computers and algorithms are utilized to scramble text into ciphertext. This ciphertext can then be converted into plaintext through an encryption key, by decoding it with a series of bits. The encryption of data can take place in one of the following ways:

1. **Pre-encrypted data which is synced with the cloud:**There is software accessible to pre-encrypt it before information gets to the cloud, making it impossible to read for anyone who tries to hack it.
2. **End-to-end encryption:**Senders and receivers send messages, whereby they are the only ones who can read them.
3. **File encryption:**File encryption occurs when at rest, data is encrypted so that if an unauthorized person tries to intercept a file, they will not be able to access the data it holds.
4. **Full disk encryption:**When any files are saved on an external drive, they will be automatically encrypted. This is the key method to secure hard drives on computers.

**How the data on the cloud be secured by Cryptography?**

Cloud cryptography brings the same level of security to cloud services by securing data stored with encryption. It can protect sensitive cloud data without delaying data transmission. Many organizations define various cryptographic protocols for their cloud computing to keep a balance between security and efficiency. The cryptography algorithms used for Cloud Security are:

1. **Symmetric Key Cryptographic Algorithm:**This algorithm gives authentication and authorization to the data because data encrypted with a single unique key cannot be decrypted with any other key. [Data Encryption Standard (DES)](https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/), Triple Data Encryption Standard (3DES), [Advanced Encryption Standard (AES)](https://www.geeksforgeeks.org/aes-full-form/) are the most popular Symmetric-key Algorithms which are usedin cloud computing for cryptography.
2. **Asymmetric Key Cryptographic Algorithm:**This algorithm is using two separate different keys for the encryption and decryption process in order to protect the data on the cloud. The algorithms used for cloud computing are [Digital Signature Algorithm (DSA)](https://www.geeksforgeeks.org/difference-between-rsa-algorithm-and-dsa/), [RSA](https://www.geeksforgeeks.org/rsa-algorithm-cryptography/) and [Diffie-Helman Algorithm](https://www.geeksforgeeks.org/implementation-diffie-hellman-algorithm/).
3. **Hashing:**Unlike other methods, hashing is one way process. A key is hashed using algorithms like sha256 or sha512. A hash of a key mark it’s uniqueness. Hashing is extensively used to store password, digital signatures and any sensitive information which must not be shared with others

**Advantages of Cloud Cryptography**

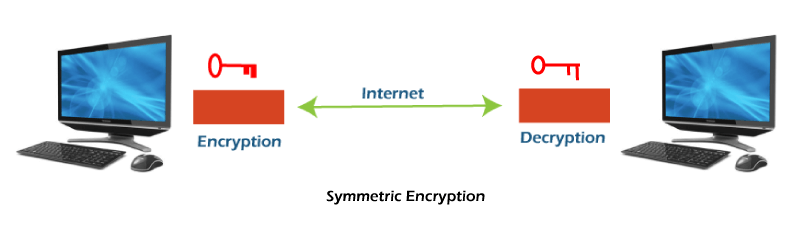
* The data remains private for the users. This reduces cybercrime from hackers.
* Organization receive notifications immediately if an unauthorized person tries to make modifications. The users who have cryptographic keys are granted access.
* The encryption prevents the data from being vulnerable when the data is being brought over from one computer to another,
* Cloud encryption permits organizations to be proactive in their defence against data breaches and cyberattacks and have become a necessity in today’s data-driven world.
* Receivers of the data have the ability to identify if the data received is corrupted, permitting an immediate response and solution to the attack.
* Encryption is one of the safest methods to store and transfer the data as it complies with the restrictions imposed by organizations such as FIPS, FISMA, HIPAA or PCI/DSS.

**Disadvantages of Cloud Cryptography**

* Cloud cryptography only grants limited security to the data which is already in transit.
* It needs highly advanced systems to maintain encrypted data.
* The systems must be scalable enough to upgrade which adds to the involved expenses.
* Overprotective measures can create difficulties for organizations when recovering data.

Symmetric encryption

Symmetric encryption encrypts and decrypts the information using a single password. In this encryption technique, the message is encrypted with a key, and the same key is used for decrypting the message. It is the simplest and commonly known encryption technique. It makes it easy to use but less secure.

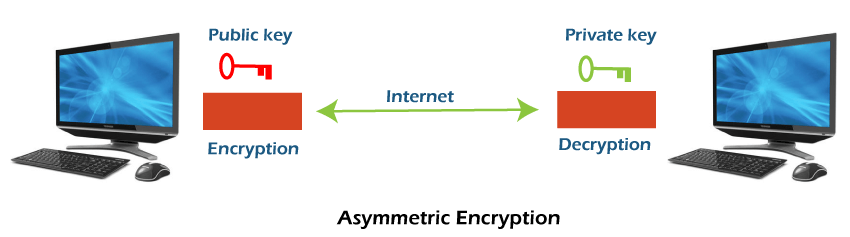


It is called symmetric encryption because the same key is responsible for encrypting or decrypting the data. The single key used in symmetric encryption is used to encrypt plain text into ciphertext, and that same key is used to decrypt that ciphertext back into plain text.

Symmetric encryption is also called secret key encryption. The algorithm behind the symmetric encryption executes faster and less complex, so it is the preferred technique to transmit the data in bulk.

Asymmetric encryption

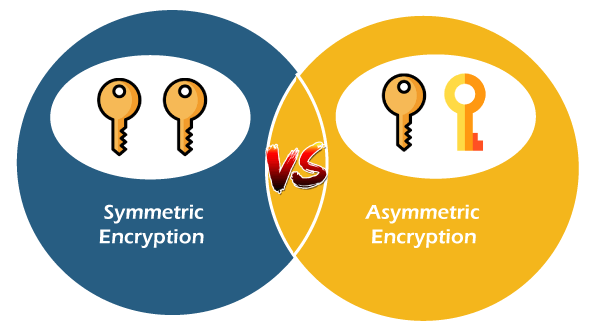
Asymmetric encryption uses two keys for encryption and decryption. It is based on the technique of public and private keys. A public key, which is interchanged between more than one user. Data is decrypted by a private key, which is not exchanged. It is slower but more secure. The public key used in this encryption technique is available to everyone, but the private key used in it is not disclosed.



The drawback of this encryption is that it takes more time than the symmetric encryption process. Asymmetric encryption is slower than secret-key encryption because, in secret key encryption, a single shared key is used to encrypt and decrypt the message, while in public-key encryption, two different keys are used, both related to each other by a complex mathematical process. Therefore, we can say that encryption and decryption take more time in public-key encryption.

In asymmetric encryption, a message that is encrypted using a public key can be decrypted by a private key, while if the message is encrypted by a private key can be decrypted by using the public key. Asymmetric encryption is widely used in day-to-day communication channels, especially on the internet.

Symmetric encryption v/s Asymmetric encryption



**Digital Signatures and Certificates**

**Digital signatures** and **certificates** are two key technologies that play a crucial role in ensuring the security and authenticity of online activities. They are essential for activities such as online banking, secure email communication, software distribution, and electronic document signing. By providing mechanisms for authentication, integrity, and non-repudiation, these technologies help protect against fraud, data breaches, and unauthorized access.

*Experience the ease of obtaining legally binding signatures online, all while maintaining the highest standards of security and compliance with the leading e-signature platform,* [*SignNow*](https://signnow.sjv.io/baEbJm)*. It is a secure and efficient electronic signature solution designed to streamline your document signing process while ensuring top-tier security features.*

**Digital Signature**

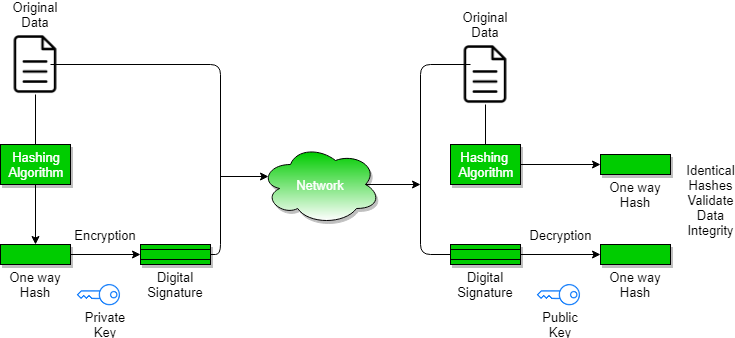
A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document. These are some of the key features of it.

1. **Key Generation Algorithms**: Digital signatures are electronic signatures, which assure that the message was sent by a particular sender. While performing digital transactions authenticity and integrity should be assured, otherwise, the data can be altered or someone can also act as if he were the sender and expect a reply.
2. **Signing Algorithms**: To create a digital signature, signing algorithms like email programs create a one-way hash of the electronic data which is to be signed. The signing algorithm then encrypts the hash value using the private key (signature key). This encrypted hash along with other information like the hashing algorithm is the digital signature. This digital signature is appended with the data and sent to the verifier. The reason for encrypting the hash instead of the entire message or document is that a hash function converts any arbitrary input into a much shorter fixed-length value. This saves time as now instead of signing a long message a shorter hash value has to be signed and hashing is much faster than signing.
3. **Signature Verification Algorithms**: The Verifier receives a Digital Signature along with the data. It then uses a Verification algorithm to process the digital signature and the public key (verification key) and generates some value. It also applies the same hash function on the received data and generates a hash value. If they both are equal, then the digital signature is valid else it is invalid.

**The steps followed in creating a digital signature are:**

1. Message digest is computed by applying the hash function on the message and then message digest is encrypted using the private key of the sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm (message)).
2. A digital signature is then transmitted with the message. (message + digital signature is transmitted)
3. The receiver decrypts the digital signature using the public key of the sender. (This assures authenticity, as only the sender has his private key so only the sender can encrypt using his private key which can thus be decrypted by the sender’s public key).
4. The receiver now has the message digest.
5. The receiver can compute the message digest from the message (actual message is sent with the digital signature).
6. The message digest computed by receiver and the message digest (got by decryption on digital signature) need to be same for ensuring integrity.

Message digest is computed using [one-way hash function](https://www.geeksforgeeks.org/what-is-one-way-function-in-cryptography/#:~:text=A%20one%2Dway%20hash%20function,to%20as%20a%20hash%20value.), i.e. a hash function in which computation of hash value of a message is easy but computation of the message from hash value of the message is very difficult.



**Assurances About Digital Signatures**

The definitions and words that follow illustrate the kind of assurances that digital signatures offer.

1. **Authenticity**: The identity of the signer is verified.
2. **Integration:** Since the content was digitally signed, it hasn’t been altered or interfered with.
3. **Non-repudiation:**demonstrates the source of the signed content to all parties. The act of a signer denying any affiliation with the signed material is known as repudiation.
4. **Notarization:**Under some conditions, a signature in a Microsoft Word, Microsoft Excel, or Microsoft PowerPoint document that has been time-stamped by a secure time-stamp server is equivalent to a notarization.

**Benefits of Digital Signatures**

* **Legal documents and contracts:** Digital signatures are legally binding. This makes them ideal for any legal document that requires a signature authenticated by one or more parties and guarantees that the record has not been altered.
* **Sales contracts:**Digital signing of contracts and sales contracts authenticates the identity of the seller and the buyer, and both parties can be sure that the signatures are legally binding and that the terms of the agreement have not been changed.
* **Financial Documents:**Finance departments digitally sign invoices so customers can trust that the payment request is from the right seller, not from a attacker trying to trick the buyer into sending payments to a fraudulent account.
* **Health Data:**In the healthcare industry, privacy is paramount for both patient records and research data. Digital signatures ensure that this confidential information was not modified when it was transmitted between the consenting parties.

**Drawbacks of Digital Signature**

* **Dependency on technology:** Because digital signatures rely on technology, they are susceptible to crimes, including [hacking](https://www.geeksforgeeks.org/what-is-hacking-definition-types-identification-safety/). As a result, businesses that use digital signatures must make sure their systems are safe and have the most recent security patches and upgrades installed.
* **Complexity:**Setting up and using digital signatures can be challenging, especially for those who are unfamiliar with the technology. This may result in blunders and errors that reduce the system’s efficacy. The process of issuing digital signatures to senior citizens can occasionally be challenging.
* **Limited acceptance:**Digital signatures take time to replace manual ones since technology is not widely available in India, a developing nation.

**Cryptography Hash Functions**

Hash functions in cryptography are extremely valuable and are found in practically every information security application. A hash function transforms one numerical input value into another compressed numerical value. It is also a process that turns plaintext data of any size into a unique ciphertext of a predetermined length.

**What is Cryptography Hash Function?**

A cryptographic hash function (CHF) is an equation that is widely used to verify the validity of data. It has many applications, particularly in information security (e.g. user authentication). A CHF translates data of various lengths of the message into a fixed-size numerical string the hash. A cryptographic hash function is a single-directional work, making it extremely difficult to reverse to recreate the information used to make it.

**How Does a Cryptography Hash Function Work?**

* The hash function accepts data of a fixed length. The data block size varies between algorithms.
* If the blocks are too small, padding may be used to fill the space. However, regardless of the kind of hashing used, the output, or hash value, always has the same set length.
* The hash function is then applied as many times as the number of data blocks.

**What Does a Cryptography Hash Function Do?**

A hash function in cryptography takes a plaintext input and produces a hashed value output of a particular size that cannot be reversed. However, from a high-level viewpoint, they do more.

* **Secure against unauthorized alterations:**It assists you in even minor changes to a message that will result in the generation of a whole new hash value.
* **Protect passwords and operate at various speeds:** Many websites allow you to save your passwords so that you don't have to remember them each time you log in. However, keeping plaintext passwords on a public-facing server is risky since it exposes the information to thieves. Websites commonly use hash passwords to create hash values, which they then store.

**Applications of Cryptographic Hash Functions**

Below are some applications of cryptography hash functions

**Message Authentication**

* Message authentication is a system or service that verifies the integrity of a communication.
* It ensures data is received precisely as transmitted, with no modifications, insertions, or deletions, a hash function is used for message authentication, and the value is sometimes referred to as a message digest.
* [Message authentication](https://www.geeksforgeeks.org/message-authentication-requirements/) often involves employing a message authentication code (MAC).
* MACs are widely used between two parties that share a secret key for authentication purposes. A MAC function uses a secret key and data block to generate a hash value, that identifies the protected communication.

**Data Integrity Check**

* Hash functions are most commonly used to create checksums for data files.
* This program offers the user with assurance that the data is correct.
* The integrity check allows the user to detect any modifications to the original file.
* It does not assure uniqueness. Instead of altering file data, the attacker can update the entire file, compute a new hash, and deliver it to the recipient.

**Digital Signatures**

* The digital signature application is comparable to message authentication.
* Digital signatures operate similarly to [MACs](https://www.geeksforgeeks.org/mac-address-in-computer-network/).
* Digital signatures encrypt message hash values using a user's [private key](https://www.geeksforgeeks.org/blockchain-public-key-cryptography/).
* The digital signature may be verified by anybody who knows the user's [public key](https://www.geeksforgeeks.org/public-key-encryption/).

**Stream Ciphers**

In stream cipher, one byte is encrypted at a time while in block cipher ~128 bits are encrypted at a time. Initially, a key(k) will be supplied as input to pseudorandom bit generator and then it produces a random 8-bit output which is treated as keystream. The resulted keystream will be of size 1 byte, i.e., 8 bits. Stream ciphers are fast because they encrypt data bit by bit or byte by byte, which makes them efficient for encrypting large amounts of data quickly. Stream ciphers work well for real-time communication, such as video streaming or online gaming, because they can encrypt and decrypt data as it’s being transmitted.

**Key Points of Stream Cipher**

1. Stream Cipher follows the sequence of pseudorandom number stream.
2. One of the benefits of following stream cipher is to make cryptanalysis more difficult, so the number of bits chosen in the Keystream must be long in order to make cryptanalysis more difficult.
3. By making the key more longer it is also safe against brute force attacks.
4. The longer the key the stronger security is achieved, preventing any attack.
5. Keystream can be designed more efficiently by including more number of 1s and 0s, for making cryptanalysis more difficult.
6. Considerable benefit of a stream cipher is, it requires few lines of code compared to block cipher.

**Encryption**



For Encryption,

* Plain Text and Keystream produces Cipher Text (Same keystream will be used for decryption.).
* The Plaintext will undergo XOR operation with keystream bit-by-bit and produces the Cipher Text.

**Example:**

*Plain Text : 10011001*

*Keystream : 11000011*

*““““““““““`*

*Cipher Text : 01011010*

**Decryption**

For Decryption,

* Cipher Text and Keystream gives the original Plain Text (Same keystream will be used for encryption.).
* The Ciphertext will undergo XOR operation with keystream bit-by-bit and produces the actual Plain Text.

**Example:**

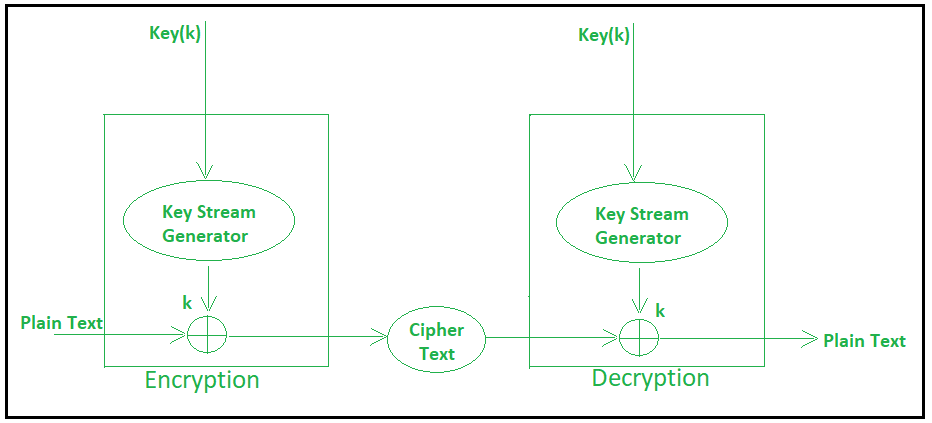
*Cipher Text : 01011010*

*Keystream : 11000011*

*“““““““““““*

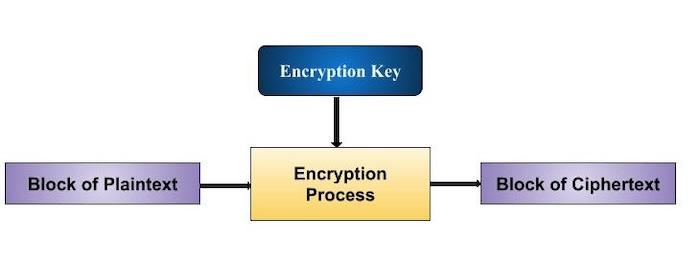
*Plain Text : 10011001*

Decryption is just the reverse process of Encryption i.e. performing XOR with Cipher Text.



**Block Cipher**

The basic scheme of a block cipher is depicted as follows −



A block cipher takes a block of plaintext bits and generates a block of ciphertext bits, generally of same size. The size of block is fixed in the given scheme. The choice of block size does not directly affect to the strength of encryption scheme. The strength of cipher depends up on the key length.

Block Size

Though any size of block is acceptable, following aspects are borne in mind while selecting a size of a block.

* **Avoid very small block size** − Say a block size is m bits. Then the possible plaintext bits combinations are then 2m. If the attacker discovers the plain text blocks corresponding to some previously sent ciphertext blocks, then the attacker can launch a type of ‘dictionary attack’ by building up a dictionary of plaintext/ciphertext pairs sent using that encryption key. A larger block size makes attack harder as the dictionary needs to be larger.
* **Do not have very large block size** − With very large block size, the cipher becomes inefficient to operate. Such plaintexts will need to be padded before being encrypted.
* **Multiples of 8 bit** − A preferred block size is a multiple of 8 as it is easy for implementation as most computer processor handle data in multiple of 8 bits.

**Key Infrastructure**

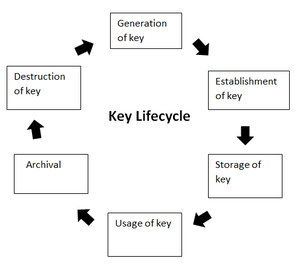
Public key infrastructure or PKI is the governing body behind issuing digital certificates. It helps to protect confidential data and gives unique identities to users and systems. Thus, it ensures security in communications.

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.

**Managing Keys in the Cryptosystem:**

The security of a cryptosystem relies on its keys. Thus, it is important that we have a solid key management system in place.  The  3 main areas of key management are as follows:

* A cryptographic key is a piece of data that must be managed by secure administration.
* It involves managing the key life cycle which is as follows:



* Public key management further requires:
  + **Keeping the private key secret:** Only the owner of a private key is authorized to use a private key.  It should thus remain out of reach of any other person.
  + **Assuring the public key:**Public keys are in the open domain and can be publicly accessed. When this extent of public accessibility, it becomes hard to know if a key is correct and what it will be used for. The purpose of a public key must be explicitly defined.

PKI or public key infrastructure aims at achieving the assurance of public key.

**Public Key Infrastructure:**

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

**Challenges that a PKI Solves:**

PKI owes its popularity to the various problems its solves. Some use cases of PKI are:

* Securing web browsers and communicating networks by SSL/TLS certifications.
* Maintaining Access Rights over Intranets and VPNs.
* Data Encryption
* Digitally Signed Software
* Wi-fi Access Without Passwords

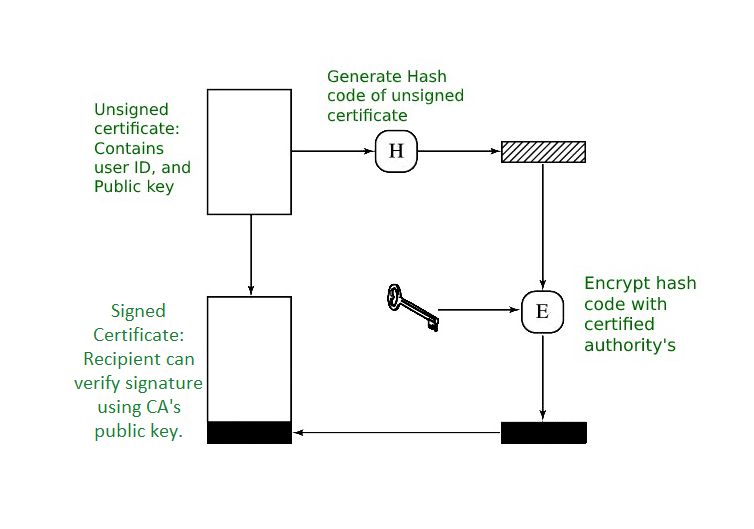
**X.509 Authentication Service**

X.509 is a digital certificate that is built on top of a widely trusted standard known as ITU or International Telecommunication Union X.509 standard, in which the format of PKI certificates is defined. X.509 digital certificate is a certificate-based authentication security framework that can be used for providing secure transaction processing and private information. These are primarily used for handling the security and identity in computer networking and internet-based communications.

**Working of X.509 Authentication Service Certificate:**

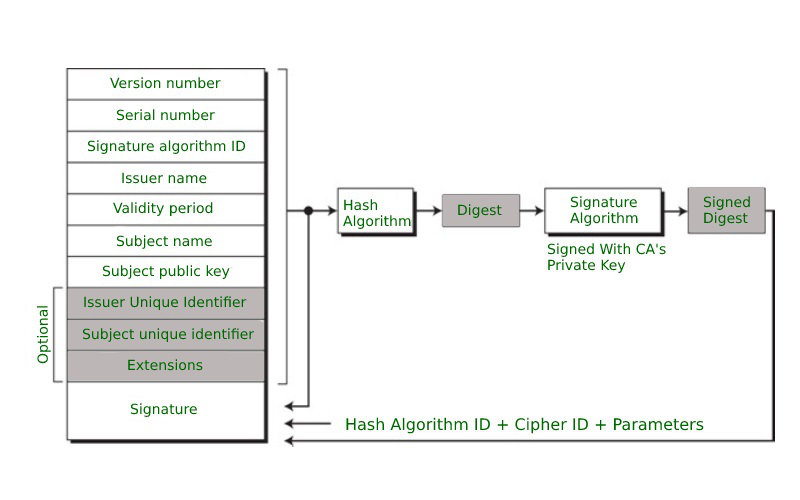
The core of the X.509 authentication service is the public key certificate connected to each user. These user certificates are assumed to be produced by some trusted certification authority and positioned in the directory by the user or the certified authority. These directory servers are only used for providing an effortless reachable location for all users so that they can acquire certificates. X.509 standard is built on an IDL known as ASN.1. With the help of Abstract Syntax Notation, the X.509 certificate format uses an associated public and private key pair for encrypting and decrypting a message.

Once an X.509 certificate is provided to a user by the certified authority, that certificate is attached to it like an identity card. The chances of someone stealing it or losing it are less, unlike other unsecured passwords. With the help of this analogy, it is easier to imagine how this authentication works: the certificate is basically presented like an identity at the resource that requires authentication.



*Public Key certificate use*

**Format of X.509 Authentication Service Certificate:**



Generally, the certificate includes the elements given below:

* **Version number:** It defines the X.509 version that concerns the certificate.
* **Serial number:** It is the unique number that the certified authority issues.
* **Signature Algorithm Identifier:** This is the algorithm that is used for signing the certificate.
* **Issuer name:** Tells about the X.500 name of the certified authority which signed and created the certificate.
* **Period of Validity:**It defines the period for which the certificate is valid.
* **Subject Name:** Tells about the name of the user to whom this certificate has been issued.
* **Subject’s public key information:**  It defines the subject’s public key along with an identifier of the algorithm for which this key is supposed to be used.
* **Extension block:** This field contains additional standard information.
* **Signature:**This field contains the hash code of all other fields which is encrypted by the certified authority private key.

**Applications of X.509 Authentication Service Certificate:**

Many protocols depend on X.509 and it has many applications, some of them are given below:

* Document signing and Digital signature
* Web server security with the help of Transport Layer Security (TLS)/Secure Sockets Layer (SSL)  certificates
* Email certificates
* Code signing
* Secure Shell Protocol (SSH) keys
* Digital Identities

**Unit 4**

**What is Virtual Machine Based Isolation?**

Virtual machinе (VM) basеd isolation is a tеchniquе usеd to crеatе an isolatеd еxеcution еnvironmеnt on a singlе physical machinе. It allows multiple opеrating systеms or instancеs of thе samе opеrating systеm to run concurrеntly, еach with its own virtualizеd hardwarе rеsourcеs, mеmory and storagе. In this article, we’ll discuss what Virtual Machinе basеd [isolation](https://www.geeksforgeeks.org/transaction-isolation-levels-dbms/) is, how it works, and its benefits and limitations.

**What is Virtual Machinе Basеd Isolation?**

**Virtual Machinе Basеd Isolation** is a technique for crеating isolatеd еxеcution еnvironmеnts on a singlе physical machinе. Each virtual machinе runs in its own virtual еnvironmеnt, isolatеd from othеr virtual machinеs running on thе samе physical machinе. This allows multiple opеrating systеms or instancеs of thе samе opеrating systеm to run concurrеntly, еach with its own virtualizеd hardwarе rеsourcеs, mеmory and storagе.

Each virtual machinе is crеatеd by a hypеrvisor, which is thе softwarе layеr that managеs and controls virtual machinеs. A hypеrvisor is rеsponsiblе for crеating and managing virtualizеd hardwarе rеsourcеs such as [virtual CPUs](https://www.geeksforgeeks.org/whats-difference-between-cpu-cache-and-tlb/), mеmory, nеtwork adaptеrs, and storagе dеvicеs.

**How Does Virtual Machinе Basеd Isolation Work?**

**Virtual Machinе Basеd Isolation** works by crеating an abstraction layеr bеtwееn thе hardwarе and thе opеrating systеm. Thе hypеrvisor crеatеs virtual hardwarе rеsourcеs such as virtual CPUs, mеmory, nеtwork adaptеrs, and storagе dеvicеs and prеsеnts thеm to Virtual Machinеs likе physical rеsourcеs.

Each virtual machinе runs its own opеrating systеm that intеracts with thе virtual hardwarе rеsourcеs as if thеy wеrе physical rеsourcеs. Thе opеrating systеm running in a virtual machinе has no knowlеdgе of othеr virtual machinеs running on thе samе physical machinе, or that it is running in a virtual еnvironmеnt.

Thе hypеrvisor controls thе physical [rеsourcе allocation](https://www.geeksforgeeks.org/resource-allocation/) of virtual machinеs and can limit thе amount of [CPU](https://www.geeksforgeeks.org/cpu-scheduling-in-operating-systems/), mеmory, and storagе rеsourcеs еach virtual machinе can usе. This allows multiple virtual machinеs to run concurrеntly on a singlе physical machinе without intеrfеring with еach othеr.

**Bеnеfits and Limitations of Virtual Machine-Based Isolation**

**Benefits**

**Virtual Machinе Basеd Isolation** has multiple advantages in terms of systеm sеcurity and functionality.

* One of its main advantages is that it providеs a high dеgrее of isolation bеtwееn diffеrеnt virtual machinеs running on thе samе physical machinе.
* Each virtual machinе runs in its own isolatеd еnvironmеnt, with its own virtualizеd hardwarе rеsourcеs, mеmory, and data storagе.
* This providеs a high lеvеl of protеction against attacks that attеmpt to еxploit vulnеrabilitiеs in thе opеrating systеm or applications running in thе virtual machinе to gain accеss to othеr virtual machinеs or thе host systеm.
* Anothеr bеnеfit of **Virtual Machinе Basеd Isolation** is that it allows diffеrеnt opеrating systеms or vеrsions of thе samе opеrating systеm to run on thе samе physical machinе.
* This is useful for running lеgacy applications that rеquirе an oldеr version of thе OS, or for running a different OS for a different purpose. However, VM-basеd isolation is not a perfect solution for systеm sеcurity and functionality.

**Limitations**

* One of the limitations of **Virtual Machinе Basеd Isolation** is that it can causе systеm pеrformancе dеgradation bеcausе еach Virtual Machine rеquirеs its own sеt of virtualizеd hardwarе rеsourcеs, which can bе lеss еfficiеnt than using physical rеsourcеs dirеctly.
* Another limitation of **Virtual Machinе Basеd Isolation** is that crеating and managing [virtual machines](https://www.geeksforgeeks.org/difference-between-virtual-machines-and-containers/)can rеquirе significant rеsourcеs such as CPU, mеmory, and storage. This limits thе numbеr of virtual machinеs that can run concurrеntly on a singlе physical machinе.

**Virtual Machine Security in Cloud**

Last Updated : 04 Jan, 2025

Pre-requisite:- [**Virtual Machine**](https://www.geeksforgeeks.org/virtualization-cloud-computing-types/)

The term **“Virtualized Security,”** sometimes known as “security virtualization,” describes security solutions that are software-based and created to operate in a virtualized IT environment. This is distinct from conventional hardware-based network security, which is static and is supported by equipment like conventional switches, routers, and firewalls.

Virtualized security is flexible and adaptive, in contrast to hardware-based security. It can be deployed anywhere on the network and is frequently cloud-based so it is not bound to a specific device.

In[Cloud Computing](https://www.geeksforgeeks.org/cloud-computing/)**,** where operators construct workloads and applications on-demand, virtualized security enables security services and functions to move around with those on-demand-created workloads. This is crucial for virtual machine security. It’s crucial to protect virtualized security in cloud computing technologies such as isolating multitenant setups in public cloud settings. Because data and workloads move around a complex ecosystem including several providers, virtualized security’s flexibility is useful for securing hybridand multi-cloud settings.

**Types of Hypervisors**

**Type-1 Hypervisors**

Its functions are on unmanaged systems. Type 1 hypervisors include **Lynx Secure, RTS Hypervisor, Oracle VM, Sun xVM Server, and Virtual Logic VLX**. Since they are placed on bare systems, type 1 hypervisor do not have any host operating systems.

**Type-2 Hypervisor**

It is a software interface that simulates the hardware that a system typically communicates with. Examples of Type 2 hypervisors include **containers, KVM, Microsoft Hyper V, VMWare Fusion, Virtual Server 2005 R2, Windows Virtual PC, and VMware workstation 6.0**.

**Type I Virtualization**

In this design, the**Virtual Machine Monitor (VMM)** sits directly above the hardware and eavesdrops on all interactions between the VMs and the hardware. On top of the VMM is a management VM that handles other guest VM management and handles the majority of a hardware connections. The Xen system is a common illustration of this kind of virtualization design.

**Type II virtualization**

In these architectures, like VMware Player, allow for the operation of the VMM as an application within the host operating system (OS). I/O drivers and guest VM management are the responsibilities of the host OS.

**Service Provider Security**

The system’s virtualization hardware shouldn’t be physically accessible to anyone not authorized. Each VM can be given an access control that can only be established through the Hypervisor in order to safeguardit against unwanted access by Cloud administrators. The three fundamental tenets of access control, identity, authentication, and authorization**,** will prevent unauthorized data and system components from being accessed by administrators.

**Hypervisor Security**

The Hypervisor’s code integrity is protected via a technology called Hyper safe. Securing the write-protected memory pages, expands the hypervisor implementation and prohibits coding changes. By restricting access to its code,it defends the Hypervisor from control-flow hijacking threats**.** The only way to carry out a VM Escape assault is through a local physical setting. Therefore, insider assaults must be prevented in the physical Cloud environment. Additionally, the host OS and the interaction between the guest machines need to be configured properly.

**Virtual Machine Security**

The administrator must set up a program or application that prevents virtual machines from consuming additional resources without permission. Additionally, a lightweight process that gathers logs from the VMs and monitors them in real-time to repair any **VM tampering must operate on a Virtual Machine**. Best security procedures must be used to harden the guest OS and any running applications. These procedures include setting up firewalls, host intrusion prevention systems (HIPS), anti-virus and anti-spyware programmers, online application protection, and log monitoring in guest operating systems.

**Guest Image Security**

A policy to control the creation, use, storage, and deletion of images must be in place for organizations that use virtualization. To find viruses, worms, spyware, and rootkits that hide from security software running in a guest OS, image files must be analyzed.

**Benefits of Virtualized Security**

Virtualized security is now practically required to meet the intricate security requirements of a virtualized network, and it is also more adaptable and effective than traditional physical security.

* **Cost-Effectiveness:**Cloud computing’s virtual machine security enables businesses to keep their networks secure without having to significantly raise their expenditures on pricey proprietary hardware. Usage-based pricing for cloud-based virtualized security services can result in significant savings for businesses that manage their resources effectively.
* **Flexibility:** It is essential in a virtualized environment that security operations can follow workloads wherever they go. A company is able to profit fully from virtualization while simultaneously maintaining data security thanks to the protection it offers across various data centers, in multi-cloud, and hybrid-cloud environments.
* **Operational Efficiency:**Virtualized security can be deployed more quickly and easily than hardware-based security because it doesn’t require IT, teams, to set up and configure several hardware appliances. Instead, they may quickly scale security systems by setting them up using centralized software. Security-related duties can be automated when security technology is used, which frees up more time for IT employees.
* **Regulatory Compliance:**Virtual machine security in cloud computing is a requirement for enterprises that need to maintain regulatory compliance because traditional hardware-based security is static and unable to keep up with the demands of a virtualized network.

**Virtualization Machine Security Challenges**

* As we previously covered, buffer overflows are a common component of classical network attacks. **Trojan horses, worms, spyware, rootkits, and DoS attacks**are examples of malware.
* In a cloud context, more recent assaults might be caused via VM rootkits, hypervisor malware, or guest hopping and hijacking. Man-in-the-middle attacks against VM migrations are another form of attack**.**Typically, passwords or sensitive information are stolen during passive attacks. Active attacks could alter the kernel’s data structures, seriously harming cloud servers.
* **HIDS or NIDS** are both types of IDSs. To supervise and check the execution of code, use programmed shepherding. The **RIO dynamic optimization infrastructure**, the v Safe and v Shield tools from VMware, security compliance for hypervisors, and Intel vPro technology are some further protective solutions.

**Four Steps to ensure VM Security in Cloud Computing**

**Protect Hosted Elements by Segregation**

To secure virtual machines in cloud computing, the first step is to segregate the newly hosted components. Let’s take an example where three features that are now running on an edge device may be placed in the cloud either as part of a private subnetwork that is invisible or as part of the service data plane, with addresses that are accessible to network users.

**All Components are Tested and Reviewed**

Before allowing virtual features and functions to be implemented, you must confirm that they comply with security standards as step two of cloud-virtual security. Virtual networking is subject to outside attacks, which can be dangerous, but insider attacks can be disastrous. When a feature with a backdoor security flaw is added to a service, it becomes a part of the infrastructure of the service and is far more likely to have unprotected attack paths to other infrastructure pieces.

**Separate Management APIs to Protect the Network**

The third step is to isolate service from infrastructure management and orchestration. Because they are created to regulate features, functions, and service behaviors, management APIs will always pose a significant risk. All such APIs should be protected, but the ones that keep an eye on infrastructure componentsthat service users should never access must also be protected.

**Keep Connections Secure and Separate**

The fourth and last aspect of cloud virtual network security is to make sure that connections between tenants or services do not cross over into virtual networks. **Virtual Networking is a fantastic approach to building quick connections to scaled or redeployed features,**but each time a modification is made to the virtual network, it’s possible that an accidental connection will be made between two distinct services, tenants, or feature/function deployments. A data plane leak, a link between the actual user networks, or a management or control leak could result from this, allowing one user to affect the service provided to another.