WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

CLOUD CRYPTOGRAPHY

Asst Pro. Ms. K. N. Rode, Miss .Mayuri Vhanmore, Miss. Sakshi Hanje, Miss. Priya Ajetrao.

Electronic &Telecommunication Engineering Department, Sharad Institute ofTechnology College Engineering Yadrav,Maharashtra, India

ABSTRACT:

Cloud computing technology is very useful in present day to day life, it uses the internet and the central remote servers to provide and maintain data as well as applications. Such applications in turn can be used by the end users via the cloud communications without any installation. Moreover, the end users' data files can be accessed and manipulated from any other computer using the internet services. Despite the flexibility of data and application accessing and usage that cloud computing environments provide, there are many questions still coming up on how to gain a trusted environment that protect data and applications in clouds from hackers and intruders.

This paper surveys the "keys generation and management" mechanism and encryption/decryption algorithms used in cloud computing environments, We proposed new security architecture for cloud computing environment that considers the various security gaps as much as possible. A new cryptographic environment that implements quantum mechanics in order to gain more trusted with less computation cloud communications is given.

Keywords: Cloud Computing, Cloud Encryption Model, Quantum Key Distribution.

Introduction:

Cryptography in the cloud employs encryption techniques to secure data that will be used or stored in the cloud. It allows users to conveniently and securely access shared cloud services, as any data that is hosted by cloud providers is protected with encryption. Cryptography in the cloud protects sensitive data without delaying information exchange.

Cryptography in the cloud allows for securing critical data beyond your corporate IT environment, where that data is no longer under your control. Cryptography expert Ralph Spencer Pooer explains that "information in motion and information at rest are best protected by cryptographic security measures. In the cloud, we don't have the luxury of having actual, physical control over the storage of information, so the only way we can ensure that the information is protected is for it to be stored cryptographically,

How does cryptography in the cloud work

Cryptography is based onencryption, in which computers and algorithms are utilized to scramble text into cipher text. This cipher text 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:

- **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.
- **End-to-end encryption-**
  Senders and receivers send messages, whereby they are the only ones who can read them.
- **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.
- **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.
- **Hashing-**
  It is mainly used for indexing and recovering items in a database. It also utilizes two separate keys for encrypting and decrypting a message.

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:

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)*, Triple Data Encryption Standard (3DES), *Advanced Encryption Standard (AES)* are the most popular Symmetric-key Algorithms which are used .

Asymmetric Key Cryptographic Algorithm-

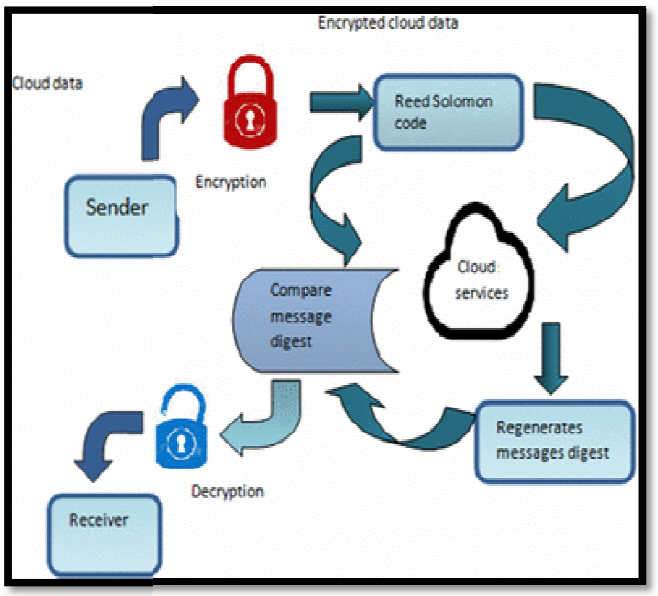
This algorithm is using two separate different keys for the encryption and decryption process in order to protect the data on the cloud. The algorithms used for cloud computing are Digital Signature Algorithm (DSA), RSA

Secure cloud data storage approach in e-learning systems

This the period of worldwide communication which is a very interesting and inspiring time in the domain of information technology. The modern daily lives may enrich based on Technical advancement in the internet sector. The gaining attractiveness of sophistication on the internet field, the creation of improved web oriented learning environment...

COVID-19, cloud adoption, infrastructure, spending, and development has been on a rapid upward trajectory. By the end of 2020, the cloud computing market was valued at around $371 billion USD, and projected to more than double by 2025.

Now that more than 90 percent of companies have adopted cloud services, and (according to some projections) more than half of all IT workloads are being handled in the Cloud, protecting data requires a “cloud first” mentality. Cloud security is a top concern for three out of every four enterprises, and the need to exploit cloud capabilities while keeping data safe has security professionals, industry analysts, and even cloud providers



How Does Cloud Cryptography Work?

There are two primary types of cloud cryptography that your organization should include in your cyber security plans: data-in-transit and data-at-rest.

Data-in-transit: - Data-in-transit is data that is moving between endpoints. A common form of data-in-transit cloud encryption is one you can see when using an internet browser: the HTTPS and HTTP protocols that secure the information channel you use when visiting different sites across the web. They do this with an SSL, or "a secure socket layer," which is a layer of encryption around the secure channel.When data is sent between your endpoint and the endpoint for the website you are visiting, the SSL within the HTTP or HTTPS encrypts your data and the website's data so that if your channel is hacked in the process, the cybercriminal would only see encrypted data.

Data-at-rest:-Data-at-rest is sensitive data you store in corporate IT structures such as servers, disks, or cloud storage services. Encrypting data while it is stored allows you to enforce access control by only giving decryption credentials to those employees with authorization. Anyone else trying to access your data-at-rest will see encrypted information rather than plaintext.

Symmetric Cryptographic Algorithm:- This type of encryption algorithm makes it possible for both data-at-rest and data-in-transit to be accessed by authorized users without manual encryption or decryption. The algorithm encrypts and decrypts the sensitive information via automatic processes once credentials are provided for authentication. Although symmetric cryptographic algorithms are usually automated, they do still require key management. keys within your organization Assure Secure Cloud Computing with ZenGRC from Reciprocity gives your security and compliance teams a streamlined, integrated dashboard experience for cyber security risk management. You can monitor known risks and receive alerts for developing attack vectors .ZenGRC's cyber security experts can help you assure the strongest level of protection for your sensitive information,

Why is Cloud Encryption Needed?

Cloud encryption is needed because its main aim is to secure and protect confidential information as it is transmitted through the Internet and other computer Systems. The best way to evaluate an organization's security and privacy status is through the CIA triad. This stands for Confidentiality, Integrity, and Availability.
Traditionally, the field of information technology only focuses on the availability of the data and its integrity. IT does not give enough thought on data confidentiality. This is why cloud encryption should be used by any organization.

Cloud Encryption Best Practices

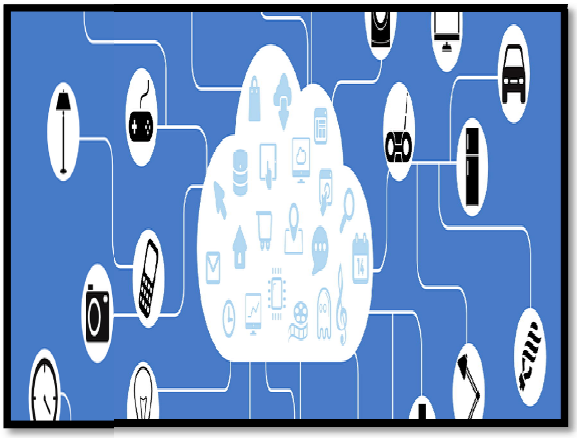
It's a top priority for an organization to keep its data protected. Just following a few preventive measures while encrypting data can strengthen its security and privacy. The following are encryption tips and best practices to protect and keep an organization's information safe in the cloud.

First, an organization should encrypt its data before uploading it. It's best to make sure to encode the data beforehand if the cloud service providers do not automatically encrypt the information. An organization can always use third-party encryption tools that provide encryption keys to files so that its data is encrypted before putting it into the cloud.

The second best practice is backing up the cloud data locally. If the data is stored in the cloud and is corrupted, an organization can always rely on locally saved versions. Choosing to store the data on a separate cloud is also a good tip. For example, if the organization is using Google Drive exclusively, it should back up important files using Dropbox.

Another tip is to secure access with cloud cryptography. Cloud cryptography is another tool to protect an organization's cloud computing architecture. Cloud computing services providers implement cryptography to provide a layer of encryption that is based on the Quantum Direct Key system. This means that this layer of information enables safe access to whoever needs shared cloud services.

Another tip to use encryption better is to protect data in transit and at rest using CASB (cloud access security broker). This is another tool to encrypt data and control encryption keys. It provides a single point of access and visibility control into any cloud app. A cloud access security broker facilitates the connections between the general public and cloud apps using proxies and API (application program interface) connectors.



Types of Cryptography

Cryptography can be broken down into three different types:

Secret Key Cryptography

- Public Key Cryptography
- Hash Functions

Secret Key Cryptography, or symmetry cryptography,

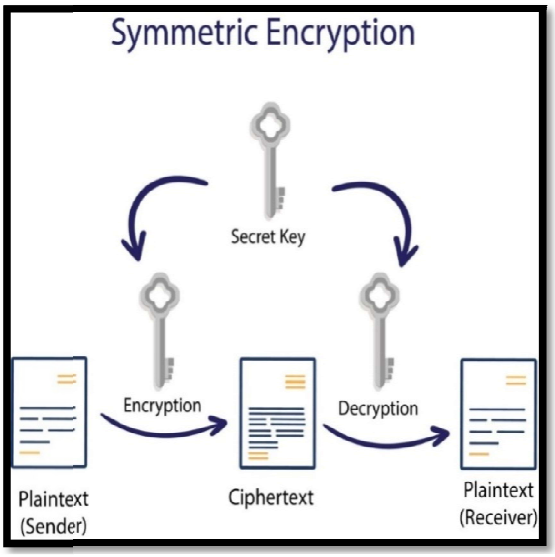
uses a single key to encrypt data. Both encryption and decryption in symmetric cryptography use the same key, making this the easiest form of cryptography. The cryptographic algorithm utilizes the key in a cipher to encrypt the data, and when the data must be accessed again, a person entrusted with the secret key can decrypt the data. Secret Key Cryptography can be used on both.

in-transit and at-rest data, but is commonly only used on at-rest data, as sending the secret to the recipient of the message can lead to compromise.

Types of Cryptography

Secret Key Cryptography

- Public Key Cryptography
- Hash Funcation



One key is kept private, and is called the "private key", while the other is shared publicly and can be used by anyone, hence it is known as the "public key". The mathematical relation of the keys is such that the private key cannot be derived from the public key, but the public key can be derived from the private. The private key should not be distributed and should remain with the owner only. The public key can be given to any other entity.

Hash functions are irreversible, one-way functions which protect the data, at the cost of not being able to recover the original message. Hashing is a way to transform a given string into a fixed length string. A good hashing algorithm will produce unique outputs for each input given. The only way to crack a hash is by trying every input possible, until you get the exact same hash. A hash can be used for hashing data (such as passwords) and in certificates.

Advantages

- The data remains private for the users this reduces cybercrime form hackers.
- Organization receive notification if an unauthorized person tries to make modification
- The users who have cryptography keys are granted access.
- The encryption prevents the data form being vulnerable when the data is being brought over from one computer to another.

Disadvantages

- Cloud cryptography only grants limited security to the data which is already in transit.
- It needs highly advanced system to maintain encrypted data.
- The system must be scalable enough to upgrade which adds to involved expenses.

CONCLUSION:

Companies and enterprises need to take a data centric approach to protect their sensitive information from advance threats in this complex and emerging environment of virtualization, cloud services, and mobility.

Companies must implement security solutions that provide consistent protection for sensitive data, including the protection of cloud information through inscription and cryptographic key-management.

REFERENCES:

1. https://www.arpatech.com/blog/what-is-cloud-cryptography
2. https://digitalguardian.com/blog/cryptography-cloud-securing-cloud-data-encryption
3. https://www.acefone.com/blog/cloud-cyptography-for-safe-transfer/
4. https://www.techtarget.com/searchsecurit