# Encryption Methods in the Cloud

Cadre
information security

# About this eBook

*“When implemented properly, cloud encryption can allow you to protect data when you don’t have full control of the environment.”-- Rich Mogull, writing for Tech Target.com.*

If you’re going to fly with the eagles in the cloud, you need to be grounded in the best cloud encryption practices. Most everyone nowadays knows the value of data backup and security. Backup is your insurance against loss; security in the wilds of the cloud is all about encryption. Is your personally identifying and proprietary data in the cloud protected by the best encryption practices?

This eBook is a layman’s guide to encryption in the cloud. Read on to learn what you should know about the basics of cloud encryption and why encryption matters. We will also touch on examples of cloud data encryption strategies, along with the basics of web data encryption and encryption key management principles.

## Encryption: The Basics

Encryption is the term for scrambling information so that only those with the key to unscrambling it can read it. Using complex mathematical algorithms, data encryption converts data to unreadable gibberish before it is moved to storage. As we shall see, encryption is analogous to putting your data in a blender to scramble it and reversing the process to restore it.

Cloud encryption transforms a cloud service customer's data into cipher text and is nearly the same as in-house encryption. There is one important difference, though: the cloud customer must know the provider's encryption standards, and, as we will discuss later on in this eBook, the provider's encryption key management practices and protocols. You can outsource cloud services and storage, but you cannot outsource your responsibility for protecting your data.

## 3 Reasons Why Cloud Encryption Matters

Reason #1 – Privacy and security concerns in the cloud are real. Encryption protects personal and proprietary information from unauthorized access and prying eyes. In 2017, data breaches approached epic proportions as hackers exposed thousands of credit card, PINs, and other personal data from companies like Verizon, Uber and Deloitte.

Reason #2 – Hackers aren't just pranksters. Big businesses, multinational outfits, and governments trying to influence foreign elections are on the prowl for personal data, business, and strategic intelligence.

Reason #3 – Laws and regulations require cloud data encryption. For example:

- Businesses and other organizations subject to the Health Insurance Portability and Accountability Act (HIPAA) must take measures to protect their patients' personal information.

Note: HIPAA data breaches have resulted in hefty fines. It is important to note that if patient data was safely encrypted but subsequently leaked, the affected organization is not required to report the breach.

- The Sarbanes-Oxley (SOX) Act protects investors from data security breaches and requires safeguarding of investors' sensitive data from fraud and abuse.
- Educational institutions must protect student data under the Family Education Rights and Privacy Act (FERPA).
- Retail businesses must adhere to the Fair Credit Practices Act (FCPA) and similar regulations.
- The credit card industry subscribes to a set of regulations known as PCI DSS (Payment Card Industry Data Security Standards). PCI DSS requires that sellers protect customers' sensitive cardholder information through good security practices and safeguarding against security breaches.

Finally, 46 out of 50 states have enacted data privacy regulations and require organizations to disclose data breaches of personal information.

## Data Encryption Standards

Although many cloud encryption standards help protect data on the cloud, the most widely accepted standards are the DES (Data Encryption Standard), AES (Advanced Encryption Standard, and RSA (Rivest-Shamir-Adleman).

**AES is the Highest Cloud Encryption Standard**

The U.S. Government National Institute of Standards and Technology oversees the Advanced Encryption Standard (AES), a formal encryption method. AES encryption employs a single, varying length encryption key. Essentially the AES Algorithm works on a single block of data and encrypts and re-encrypts it 10 to 14 times, depending on the length of the key.  AES meets all U.S. Government requirements for protecting health, (HIPAA) and financial data security.

**DES is published by the National Institute of Standards (NIST)**

This standard employs a single, secret key for both encrypting and decrypting data. Working on 64 bits of data at a time it uses a 56-bit key. Its output is scrambled text in blocks of 64 bits.

**RSA is the most popular asymmetric algorithm**

Developed in 1977, this encryption method is still used today in hundreds of software products and encryption key exchanges. It is mainly used for secure open-channel communications.

## Encryption Keys are Symmetric and Asymmetric

An encryption key is a like a password on steroids. It is a completely random and unique string of characters designed by computer algorithms. Each key is both unique and unpredictable.

**1. Symmetric Keys are for data at rest**

This type of key cryptography uses the same key to encrypt and decrypt the data. It is used mainly to encrypt sensitive data while the data is stored in a database, for example. Symmetric keys also decrypt the data into plaintext when a user accesses it.

**2. Asymmetric keys are for data in motion**

Asymmetric keys are a different pair of keys for data encryption and decryption. Asymmetric keys are both of the private and public varieties:

- **A public key** encrypts the data and is freely given, because it encrypts data, rather than decrypting it.
- **A private key** decrypts data that the public key has previously encrypted. This key must be safeguarded for obvious reasons.

## Architecture and Methods of Cloud Data Encryption

TechTarget contributor, Rich Mogull, describes three common security architectural arrangements:

**1. Encrypting the data before it is sent to the cloud in a private storage arrangement**

When the data is downloaded, it is decrypted. This method is suitable for cloud backup. The data goes to the cloud without the encryption keys, which are stored locally. (More on encryption keys later in this eBook…)

**2. Writing a new encryption volume each time you use the application**

The data is stored in a second encrypted volume and protects the user from unauthorized access during a particular instance of online activity.

**3. Separating the encryption key from the encryption engine during the cloud access session.**

Some special cloud encryption products only return the encryption key, after manual approval of a new run, for example.

## Cloud Data Encryption for Web Access: The Basics of SSL and VPNs

A secure form of cloud data encryption is through what is known as an SSL (Secure Socketss Layer). This is a form of data encryption as the data goes to and from a website. It blocks hackers from seeing and interfering with the data in transit. A website protected by SSL has a green padlock icon in the URL bar and the web address begins with “HTTPS.”

SSL provides security as a local browser tries to connect. The browser requests the web server to identify itself, whereupon the web server transmits its SSL verified certificate for checking and approving of the server’s credentials. If the credentials are valid, a secure and encrypted exchange of data ensues.

VPN stands for “virtual private network.” VPNs provide secure, encrypted access points for server or website users. VPNs connect to public networks and provide a secure two-way connection and interface between the user and the information the user is accessing. This is an additional layer of cloud security, since individual users can rely on VPNs to protect their identities during cloud sessions. The VPN, in turn, will permit a website to collect data that the user on the other end has allowed.

## Cloud Encryption Key Management is “the Key”

Protecting and managing encryption keys is, for obvious reasons, critical to successful encryption on the cloud. The process requires generating, exchanging, storing, using, securely shredding, and replacing encryption keys. Said keys are analogous to safe combinations. So, a robust encryption key management must include policies, protocols and procedures for:

- Managing the lifecycle of the encryption key
- Controlling physical and logical access to servers where the key data are stored
- Designating user/role access to encryption keys

## Conclusion

This has been a basic (and non-technical) description of methods and tools used for cloud encryption. Your takeaway is this: before you park personal or sensitive data on the cloud, make sure that whoever is storing it for you is using a level of cloud encryption that will protect you from a data breach that could ruin your day and close your business.

A short bibliography for further non-technical reading:
*What is Encryption, and How Does It work?* by Zainul Franciscus—A non-technical guide to encryption.

*Using Data Encryption in the Cloud - A* Business.com guide to effective data protection, along with suggestion on safeguarding encryption keys.

*VPN Encryption Guide: And How It works* - A clever rundown of VPN methods and technology.