KEEPING YOUR DATA SAFE IN THE CLOUD

THE ULTIMATE AMAZON WEB SERVICES ENCRYPTION GUIDE

"ENCRYPTION IS A KEY MECHANISM FOR CUSTOMERS TO ENSURE THAT THEY ARE IN FULL CONTROL OVER WHO HAS ACCESS TO THEIR DATA."

- WERNER VOGELS, CTO, AMAZON CLOUD

NetApp®

Table of Contents

Executive Summary

Panama Papers captured headlines when it leaked a record high of 11 million documents and 2.6TB of data belonging to tax avoidance and offshore company specialist Mossack Fonseca. It wasn't the first megaleak - think Wikileaks Cablegate, Ashley Madison, and Sony Pictures - but its predecessors were nowhere near as large. Vast amounts of damaging data spewed forth, exposing the questionable practices of the powerful and famous.

For example, it exposed how the prime minister of Iceland failed to disclose his wife's offshore firm, which had a claim on failed banks, and how the father of UK Prime Minister David Cameron was running an offshore company to avoid taxation. Such incidents call into question the security of sensitive data again and again.

> In simple terms, encryption can be defined as securing or protecting your information from unauthorized access. Encryption involves the conversion of sensitive information into a ciphertext using an algorithm.

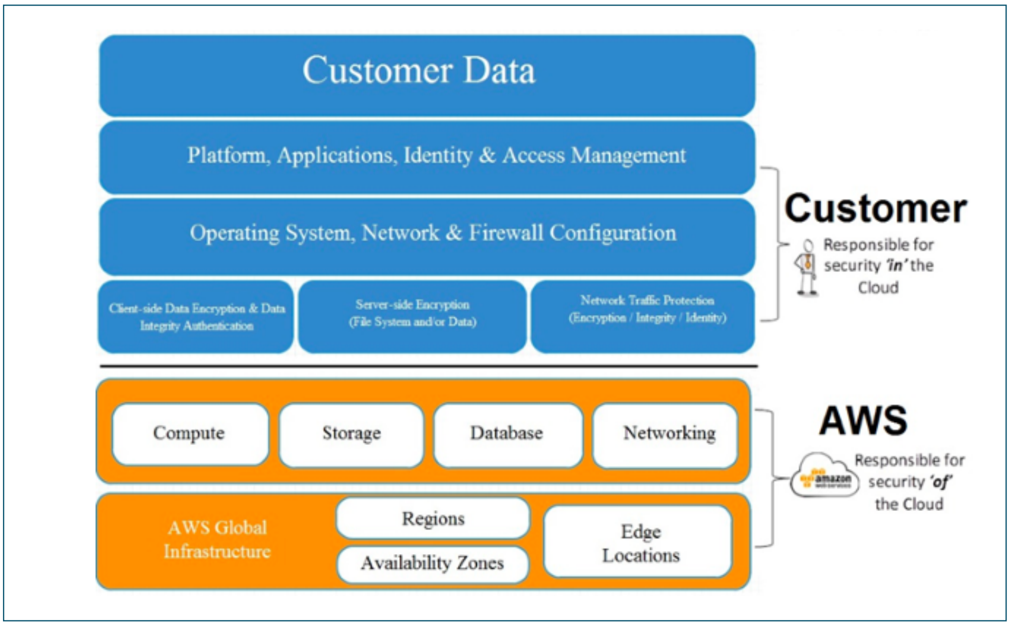
The reverse process of decryption takes the ciphertext and converts it back into the original format. During this process, the encryption algorithm and key are known only by the source and destination.

Nowadays, encryption is required everywhere, from small static websites running on a public cloud service all the way to enterprise-grade services. Additionally, almost every site can accommodate an SSL certificate and some level of back-end data encryption. As your enterprise moves to the cloud, in particular to Amazon Web Services (AWS), you need to be able to quickly learn the hows and whats of data encryption in the public cloud.

This paper will help you understand the key concepts of encryption in the cloud and dive into the services and tools that AWS enterprise users can use to protect their data.

Cloud Shared Responsibility Model

With the evolution of public clouds and the migration of traditional data center workloads to the cloud, it is important to make sure that your sensitive information is safe and secure. Public cloud providers work with a shared responsibility model. This shared responsibility model says that “public cloud vendors are responsible for the security *of* the cloud” and “the customer is responsible for security *in* the cloud.”


Customer Data
Platform, Applications, Identity & Access Management
Operating System, Network & Firewall Configuration
Client-side Data Encryption & Data Integrity Authentication
Server-side Encryption (File System and/or Data)
Network Traffic Protection (Encryption / Integrity / Identity)
Customer
Responsible for security 'in' the Cloud
Compute
Storage
Database
Networking
AWS Global Infrastructure
Regions
Availability Zones
Edge Locations
AWS
Responsible for security 'of' the Cloud

The above image shows that anything below the hypervisor level, including hypervisor security, servers, racks, power supply, and the Internet, is completely the responsibility of the cloud provider (that is, AWS). Anything above the hypervisor (that is, the operating system, network, firewall configurations, applications, and encryption) **is completely your responsibility**.

Public cloud providers such as the IaaS market leaders - Amazon Web Services and Microsoft Azure - have already made their environment secure. From your perspective, encryption on the infrastructure level is totally seamless, especially the networks (that is, LAN, WAN) and storage.

The public cloud vendors made these commonplace as a bundled element in their offerings and have already met multiple compliance standards, but this doesn’t free you from liability to your own users.

This article will help you take action when it comes to your responsibility for maintaining a secure and compliant cloud environment.

Encryption: Cloud Basics

Server-Side vs. Client-Side Encryption

The key differentiator between server-side encryption and client-side encryption lies in the answer to these two questions:

Where are my encryption data and keys stored?

Who is responsible for managing the keys?

If the encryption key is stored and managed by the cloud provider, that means server-side encryption where you rely on your provider's security and audit controls.

Although provider-managed encryption removes the hassle and complexity in isolating your data from your end, for regulated workloads, encryption and key management are still your responsibility.

In the cloud, client-side encryption is the preferred method because you manage the keys, meaning you retain complete control over your data.

Though public cloud vendors such as Amazon are strict when it comes to their customers' data, client-side encryption eliminates the possibility of the data being viewed by your provider and makes sure it can be viewed by your end users only.

Encryption in AWS

Key Management

In order to fulfill your side in the shared responsibility equation, you should be able to safely manage and store the encryption key.

> Using AWS, key management can be done on three different levels:
>
> 1. Rely on AWS to administer and maintain the keys
> 2. Use Amazon Key Management Server (using KMS and CloudHSM)
> 3. Use an on-premises key management server solution

1. AWS Key Management Service (KMS)

AWS Key Management Service (KMS) is a managed solution that allows you to create and manage your encryption keys. The service integrates natively with various other AWS data and storage services, such as S3, RDS, EBS, Elastic Transcoder, Workmail, and Redshift.

KMS is based on the concept of an envelope algorithm, so it requires multiple keys to encrypt and decrypt confidential information (that is, a data key to encrypt the data and your master key to encrypt the data key). In addition, KMS tight integration with AWS CloudTrail allows you to keep an audit trail of your account, making sure that all actions related to KMS are recorded for compliance purposes.

Following are two KMS main features of which you should be aware.

1. Customer Master Key

   The AWS customer master key (CMK) encrypts the data keys and stores them in a secure vault that can't be exported. It provides us with the ability to manage the permissions of who can administer and use these keys. The keys are unique for the account and region. There are two types of master key: AWS-managed master key and customer-managed master key.

   The AWS-managed master key is offered with most AWS services, allowing users to use them directly. These keys don't provide the key rotation capabilities. In contrast, customer-managed master keys can be created and managed by the client and offer key rotation capabilities as well.

2 Data Key

The data key is used for data encryption and has export capacity. AWS does not store, manage, or track your keys. The data is encrypted using a plaintext data key, and data keys are encrypted using the CMK.

On performing decryption, the encrypted data key is converted into a plaintext data key using CMK; the key is later used to decrypt the data. AWS KMS is used to generate, encrypt, and decrypt data keys but does not manage, store, or track their usage. The ownership and responsibility for management, storage, and tracking of the data keys lie solely with the application owner.

2. AWS CloudHSM

AWS CloudHSM is a dedicated, tamper-proof, hardware appliance solution to provide secure key storage and cryptographic operations to meet corporate, contractual, and regulatory compliance requirements. The key concerns for the regulatory workload organization in migrating an application to the cloud are key management, application performance, and availability.

CloudHSM uses Luna SA 7000 HSM appliances from SafeNet with version 5 of the Luna SA software and Luna clients deployed on the EC2 instances.

As the HSM device models comply with various international and U.S. government regulatory standards, for example, NIST FIPS 140-2, the key management is taken care by CloudHSM. CloudHSM has already been validated and is compliant with the Payment Card Industry (PCI) Data Security Standard (DSS).

To ensure similar application performance, the CloudHSM appliance is placed inside the same VPC as the application and data it protects, making sure of low-latency connectivity and performance of the EC2 instances.

Lastly, AWS CloudHSM is available in multiple regions and availability zones to make sure of high availability of the applications. It’s important to note that you can use AWS CloudTrail integration to CloudHSM to record all API calls and logs saved in Amazon S3.

Apart from EC2 instances, AWS CloudHSM can be used with Amazon Redshift, Amazon RDS Oracle, and third-party applications such as Microsoft SQL Server or Apache.

Various cryptographic libraries are available, such as PKCS 11 and Java JCA/JCE, that allow developers to integrate CloudHSM with their applications.

3. Using an External Key Manager

Traditional data centers are composed of various custom hardware and software. When it comes to encryption, virtual key management appliances are used to secure storage repositories and management of the encryption keys.

Due to various regulatory and hybrid workloads, enterprises try to avoid putting "all their eggs in the same basket," meaning that your key management appliance should reside outside of the public cloud to make sure that the different segmented networks are behind additional security layers. In this case, the key management server would be located on your premises and would manage both environments.

To preserve application performance and make sure of security in transit, integration between AWS and an on-premises key manager is carried out over a secure hybrid network, using either AWS VPC or AWS Direct Connect.

> This external key manager requires the availability of various cryptographic libraries so that the application can use them to encrypt and decrypt the data.

These external key managers can interact with an AWS CloudHSM as well.

In addition, various external key managers are available on AWS Marketplace. While AWS KMS service only offers Advanced Encryption Standard (AES) encryption algorithms, the external key managers provide various data encryption algorithms such as AES, Data Encryption Standard (DES), and Triple DES (TDES), which are approved by various compliance and government bodies.

In-Transit Encryption

Encryption in transit is more aligned with network-level encryption, making sure that the network traffic is completely secure and all information transmitted over it is encrypted. In the event of snooping, the information remains secret and is junk to the snooper.

In the cloud world, any confidential traffic flowing between various layers in your infrastructure or leaving your public cloud needs to be encrypted. Later in this article, we'll discuss the Amazon options and offer examples of how this comes into play when planning your cloud architecture for compliance with the Health Insurance Portability and Accountability Act (HIPAA).

Running on AWS, you should use elastic load balancing (ELB) to terminate and process web sessions containing sensitive information. If you need all your network traffic to be encrypted in transit end to end, you have two options: terminate HTTPS or HTTP/2 over TLS and terminate SSL/TLS on an ELB.

This encrypted data streams between the end client and the ELB. The second option is carried out by configuring the ELB in basic TCP mode or over WebSockets and moving encrypted information to back-end instances. In this architecture, you need to own and manage certificates and TLS policies yourself.

You should also check out AWS Certificate Manager, which is a service that allows you to provision, deploy, and maintain SSL/TLS. This native AWS tool facilitates certificate deployment on top of an ELB or CloudFront. What's more, it is free.

Third-Party Services

Ready for the Next Step?
Start Your 30-Day NetApp ONTAP Cloud for AWS Trial

Apart from the native AWS solutions, there are various third-party and open-source tools that allow you to encrypt data at rest and in transit. You might prefer these solutions to align your security controls in a hybrid or multicloud environment.

This can be an easy solution if you already run an on-premises data and storage solution that is already secured by your enterprise vendor. Instead of implementing a whole encryption solution, just rely on your vendors to seamlessly expand their capabilities across the clouds, allowing them to keep your data seamlessly encrypted in the public cloud.

You can look at open-source solutions, such as Hashicorp's Vault. Or enter the AWS marketplace storage solutions and look for ONTAP® Cloud, which can help keep encrypted data in sync between your on-premises data center and AWS cloud at all times using NetApp® SnapMirror® technology.

Use Case: HIPAA Compliance on AWS

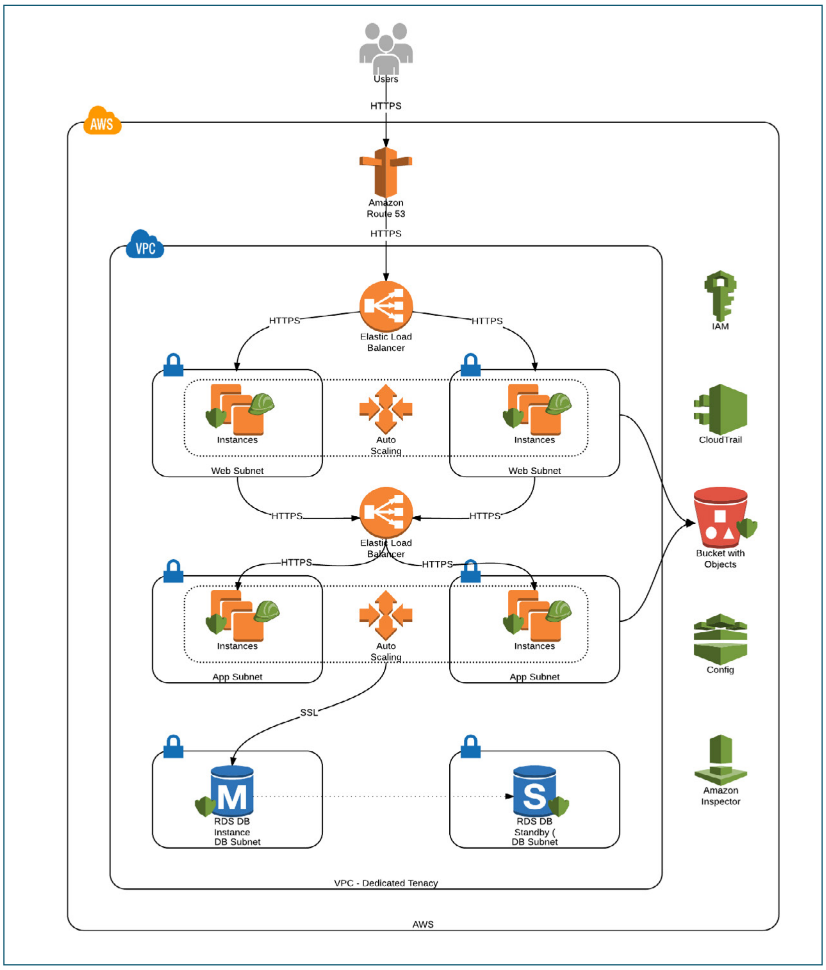
HIPAA deals with protecting the security and privacy of personal health information (PHI), which contains sensitive, health-related information of employees. The act also makes sure employees retain their insurance coverage when they change workplaces or lose their jobs.

One of the main rules of HIPAA is that any PHI data in transit or at rest must always be encrypted. For that purpose, AWS is considered as the reliable platform for deploying HIPAA application.

An easy deployment of a HIPAA-compliant web application on AWS can use EC2 dedicated instances (using either dedicated tenancy VPC or dedicated EC2 instance in default tenancy VPC) with KMS-encrypted EBS volumes.

For in-transit encryption of all requests between instances, you should use elastic load balancers (ELBs) and enable SSL termination to build end-to-end encrypted links. In particular, make sure that all communication with the back-end layer is encrypted using the ELB back-end authentication feature.

For the database, you can leverage Amazon RDS service with encryption enabled. It is important to make sure that none of the PHI data is stored in the database in plaintext form. The data should be encrypted at the application level, leveraging AWS KMS or other solutions, as applicable for any PHI data in a database or file system.



In the above HIPAA-compliant architecture, Amazon VPC with dedicated tenancy is used. All traffic is encrypted in transit with SSL termination, and back-end authentication is enabled at the ELB layer. The communication between the web layer and app layer is also encrypted with an internal ELB layer used between them. All the instances in the web layer and app layer are using KMS-encrypted EBS volumes. The database is again encrypted using AWS KMS service.

It's important to note that if you build a compliant environment on AWS, you need to validate and consider only services that are certified for the specific standard.

For our case, as of now, only 11 AWS services are considered to be HIPAA compliant. For further information, check out how to architect HIPAA on top of AWS.

Final Notes

> “AWS encryption solutions are for all. That is, they fit startup to midscale to enterprise workloads, Amazon-specific workloads, and hybrid workloads. Whether migrating to the cloud or starting a new mobile app running completely on AWS, you will end up with a pile of data and files that only grows over time.”

You should map and define which of your applications require a higher level of security and privacy. This will allow you to focus on the relevant data subsets - specific databases, tables, storage repositories, or folders or files - and make sure they are encrypted.

The choice of the encryption solution depends upon the security and compliance standards requirements of your organization. We hope that this paper helped you understand your options when it comes to the cloud.

About NetApp ONTAP Cloud for AWS

ONTAP Cloud, the leading enterprise storage operating system, is deployed using OnCommand® Cloud Manager to deliver secure, proven NFS, CIFS, and iSCSI data management for AWS EBS storage. A software-only storage service running NetApp ONTAP software, ONTAP Cloud combines data control with enterprise-class storage features such as data deduplication and compression to minimize your EBS storage footprint.

You can take Snapshot® copies of your data without requiring additional storage or affecting your application's performance. And ONTAP Cloud can tie your Amazon cloud storage to your data center using the leading NetApp replication protocol, SnapMirror technology.

To enhance your data security, ONTAP Cloud offers encryption of your at-rest storage managed by NetApp, while you retain the encryption keys. Global enterprises and government customers rely on NetApp storage security solutions to protect their data with the strongest security technologies available.

The ONTAP Cloud storage security solution helps prevent unauthorized modification or disclosure of data stored across your enterprise, supporting your key data security and compliance initiatives.

It will help you address:

- Data privacy requirements
- Regulatory compliance
- Cloud storage
- Secure storage consolidation
- Multitenant solution providers
- Secure backup
- Intellectual property protection
- Secure information sharing

To find out more, visit cloud.netapp.com.

Start Your 30-Day NetApp ONTAP Cloud Trial for AWS

amazon web services

NetApp