Tech Insight: Cloud Encryption

Volume 6, Issue 7
Office of Information and Technology (OIT)

In a past issue of *Tech Insight*, "Guide to Encryption," we explored the history, digital data states, benefits, and challenges of how the Department of Veteran Affairs (VA) utilizes encryption. With increased hacking from multinational organizations and rogue state agents, information security challenges remain a primary focus of government and industry leaders. VA is required to ensure that its security features protect the sensitive information of our nation's Veterans—information that is included in the data packets that pass through the unknown servers, routers, and devices of the internet, before they arrive to their authorized recipients. This *Tech Insight* explores an overview of cloud encryption; its benefits, challenges, and best practice approaches to implementation; and how cloud encryption is used at VA.

Overview

Encryption was known before the digital age as *cryptography*. It involves converting unencrypted data, referred to as *plain text*, into another form, referred to as code or *ciphertext,* by using an algorithm called a *cipher*. Encryption guards digital data privacy as the code is stored on computer systems and sent via the internet and other networks. The ciphertext message contains all the information of the plaintext message, except that is not in a format that is readable by a human or computer—it is meaningless if it is accessed without authorization. Finally, the code becomes only readable to those who have access to its secret key, known as the *decryption* key, or password. If the same key is used to encrypt and decrypt on both sides, the encryption is called *symmetric*. Although symmetric encryption is very fast, it may be vulnerable to interception when the key is passed from the sender to the recipient. On the other hand, *asymmetric* encryption, often referred to as *public key*, uses two types of keys—a public key and a private key, with the private key only revealed to the recipient.

Cloud encryption services are offered by cloud storage providers to encrypt data before it is transmitted to the cloud for storage. Generally, cloud encryption applications range from

encryption connections to only a *limited* encryption of data that is identified as sensitive (i.e., account credentials), to *end-to-end* encryption of any data that is transferred to the cloud. End-to-end encryption is an implementation of asymmetric encryption. As the name implies, end-to-end encryption protects data most effectively, since it can only be read on two ends, by the sender and by the recipient. Cloud storage providers encrypt data in these models by passing encryption keys to customers.

The main idea of any encryption process is to keep sensitive data secret from other users by processing readable information into long series of random or pseudo-random ciphers. Encryption is known to be one of the most efficient methods of securing data, since organizations can be certain that only those who are authorized will have access to sensitive information. Without encryption, any piece of data or message is readable by anyone who is able to intercept data in transit or steal data stored on servers.

Benefits and Challenges

The main benefit of cloud encryption is identical to any application of encryption: encrypted data is readable for authorized individuals with access to the decryption keys. If the data is misplaced, no one can access it if its keys remain secure. This is particularly advantageous when data is being stored in the cloud, as the cloud guards data in the event that a provider, account, or system is compromised.

For enterprises that need to meet regulatory compliance requirements, cloud encryption is vital. When combined with other security measures, encryption permits organizations to meet the strict compliance requirements of the Health Insurance Portability and Accountability Act (HIPAA) for healthcare organizations and business associates, the Payment Card Industry Data Security Standard (PCI DSS) for e-commerce and retail enterprises, and the Sarbanes-Oxley Act (SOX) for financial reporting. Any enterprise within these industries that has implemented the cloud must be prepared to meet the required compliance measures. Cloud encryption is used as a line of defense for data breaches and cyberattacks.

A primary challenge with encryption is that it is underutilized, even with proven success at strengthening data security. However, as more organizations request increased security measures from cloud providers to improve compliance while sustaining productivity, utilization has become more prevalent.

Encryption increases costs for cloud storage providers due to the extra bandwidth that is necessary to encrypt data before it is transmitted to the cloud. As an outcome, some providers cap their cloud encryption services, with cloud storage customers encrypting their own data on site before transferring to the cloud. Few cloud consumers choose to encrypt their own data, since keeping the total encryption process and all keys within their setting can be less costly.

Best Practices for Cloud Encryption

When selecting a cloud storage provider, it is important to chart security needs for cloud deployment and any data that will be pushed to the cloud. Classify the data that needs to be encrypted and choose a cloud provider that can adequately provide encryption. For instance, a marketing team using cloud storage for graphics and videos might need encryption for their account identifications, but not for any information transmitted to the cloud. However, manufacturers and engineers using cloud storage services to share source code and map documents will most likely demand cloud providers with end-to-end encryption. At a minimum, select cloud providers that use Hypertext Transfer Protocol Secure (HTTPS) to make sure all connections are encrypted. When possible, sensitive data sent to the cloud should be encrypted on site, before uploading. This guarantees that data will be protected in the cloud even if the account or cloud storage provider is vulnerable.

Secure encryption key management[1] is crucial. Encryption keys must be stored apart from the encrypted data to safeguard data security. Additionally, key backups should be kept offsite and audited frequently. Another encryption best practice is to intermittently refresh keys, especially if keys are set to terminate automatically, as few organizations choose to encrypt their own keys. Another best practice is to apply multi-factor authentication for both the recovery and master keys.

Business regulations and data security requirements become a necessity when challenges are presented with cloud encryption. Privacy and data security experts acknowledge that encryption is a critical instrument for information security, and cloud providers provide various applications of encryption to fit a series of data security requirements and budgets. Researching the encryption services offered by an array of cloud vendors, planning for secure cloud adoption, and taking the time to comprehend cloud data protection needs will allow business to advantage of the benefits of cloud storage and computing without putting data at risk.

Cloud Encryption at VA

Cloud encryption is evident throughout several areas at VA. Virtru, a data privacy and protection firm, is currently used by VA to protect email, whether it's shared from Microsoft Office 365 or other email providers. The Department needed to share material across its network of providers and with Veterans but did not have adequate encryption technology to meet government regulations. Prior to Virtru, VA used faxes and couriers to share personal health information, which detracted from its ability to deliver efficient care to Veterans.

Mobile data security is also very important at VA. The Veterans Health Administration (VHA) Healthcare Security Requirements (HCSR) Office reviews mobile applications[2] to make sure they

[1] Townsend Security, "The Definitive Guide to Encryption Key Management Fundamentals," https://info.townsendsecurity.com/definitive-guide-to-encryption-key-management-fundamentals
[2] VA Mobile, Data Security, https://mobile.va.gov/content/data-security

follow VA software data security standards. The HCSP ensures that if the application is created to transmit, store, or process a Veteran's electronic protected health information (PHI) and personally identifiable information (PII), it has the proper security control protocols to encrypt stored clinical information with the Federal Information Processing Standard (FIPS) 140-2 validated encryption; and encrypt data transmitted to or from VA with FIPS 140-2 validated encryption.

Microsoft Azure Government cloud was approved to store the Department's most sensitive data. Moreover, in 2017, the Federal Risk and Authorization Management Program confirmed that Azure met the security requirements needed to handle VA's "sensitive data, including personally identifiable information (PII) and protect health information (PHI)."

Furthermore, based on the engineering guidance established by the VA Enterprise Cloud Solutions Office in support of the VA Enterprise Cloud Concept of Operations (CONOPS), Azure Storage automatically encrypts data prior to storage and decrypts prior to retrieval; the encryption, decryption, and key management are transparent to users. Remote Key Management and Client-Side Key Management are common approaches to management in the cloud. Azure provides cloud based key management services for managing keys to support cloud usage. By using Microsoft Azure Key Vault, keys and secrets (such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords) can be encrypted using keys that are protected by hardware security modules (HSMs). Additionally, keys can be generated or imported into the HSMs.

Conclusion

Sensitive data is moving to the cloud at an extraordinary pace and enterprises are seeking ways to extend encryption policy controls. Cloud encryption is mainly driven by the need to encrypt data before it is transmitted to the cloud for storage. Encryption makes information indecipherable to users without access to the encryption keys, but when a cloud provider encrypts the information, administrators at the provider can view the data.

By the end of 2025, the global cloud encryption market will be worth $2.9 million, according to a report[3] by Transparency Market Research (TMR). North America has been the key leader in the market for cloud encryption. For more information on encryption, read *Tech Insight:* "Guide to Encryption." To read more about key service management and the VAEC, read the GovCloud Deployment Model Enterprise Design Pattern (EDP) and Migration Framework EDP. To learn more about other new technologies surfacing across VA, visit our *Tech Insight* page.

The Tech Insight Series

The monthly *Tech Insight* series aims to help readers make better decisions and be more informed customers of OIT products and services by providing them with high-level overviews of technologies that impact or will impact

[3] TMR, Cloud Encryption Market, https://www.transparencymarketresearch.com/cloud-encryption-market.html

VA's IT environment. Each *Tech Insight* introduces topics in an easily digestible fashion by presenting background information on the topic, clearly explaining its importance within VA, and providing recommendations for success from OIT. Access all *Tech Insights*.

Disclaimer: *This document includes links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.*