Estudio del desempeño de algoritmos de criptografía para almacenamiento de archivos encriptados en la nube

Dilan Esteban Rey Sepulveda 2190397 Sergio Hernando Barón Rivera 2201885

Universidad Industrial de Santander

Introducción

La computación en la nube ser refiere al uso del software de infraestructura en red y la capacidad que proporciona recursos al entorno bajo demanda. La complejidad de la nube se púede reducir a miles de primitivas y unidades funcionales comunes replicadas. Estas componentes más simples crean muchos problemas relacionados con la seguridad. EL desafío de los problemas de seguridad surge debido al hecho de que tanto los datos del cliente como del programa residen en las instalaciones del proveedor.

Este articulo desarrolla una evaluación de 2 técnicas/algoritmos de cifrado seleccionadas, a saber, Fernet (de la librería cryptography de phyton)y el cifrado Cesar. La evaluación del desempeño de estos algoritmos se realiza midiendo el tamaño resultante del archivo después de encriptar/desencriptar y a su vez el tiempo que toma cada algoritmo para realizar estos procesos, esto en ambos ambientes de ejecución (nube y local).

El objetivo principal de este articulo es investigar y estudiar distintos tipos de algoritmos que se pueden implementar en una nube de Amazon Web Services (AWS) para un microservicio de almacenamiento de documentos confidenciales.

Computación en la nube

Aspectos importantes

Los aspectos más importantes del Cloud Computing incluyen:

- Acceso a demanda
- Escalabilidad
- Servicios Medibles y Gestionados
- Acceso ubicuo
- Modelo de pago por uso
- Servicios Compartidos
- Elasticidad

Seguridad de la computación en la nube

Existen importantes preocupaciones de seguridad que deben abordarse al considerar trasladar aplicaciones críticas y datos confidenciales a entornos de nube públicos y compartidos. Para abordar estas preocupaciones, se debe desarrollar controles suficientes para proporcionar el mismo o mayor nivel de seguridad que el que tendría la organización si no se utilizara la nube.

Metodología

Proceder

Se utilizará una instancia de Amazon Web Services conocida como EC2 t2.micro (capa gratuita AWS) con un SO Ubuntu Server 22.04. La conexión remota a la instancia se realiza mendiante SSH usando el programa MobaXTerm. Se codifican los distintos algoritmos en programas .py, cada uno para su respectivo proceso (Encriptar o Desencriptar).

Recursos

- Instancia AWS EC2 t2.micro con un vCPU Intel Xeon Scalable de hasta 3.3 GHz, 1 Gib memoria. Sitema operativo instalado: Linux Ubuntu Server 22.04
- Local: Intel core i5-8300H 2.30GHz, 4 procesadores físicos, 8 lógicos, 16 GB Memoria. Sistema operativo instalado: Windows 10.

Algoritmos

- Fernet(Libreria 'cryptography' de Python): Es una implementación de criptografía autenticada simétrica(clave secreta)
- El método César: Es un algoritmo de cifrado muy simple que se basa en desplazar cada letra de un texto una cantidad fija de posiciones en el alfabeto.

Archivos utilizados

- lorem.txt (Tamaño:6kb)
- titanic.csv (Tamaño:59kb)

Experimentos (Resultados)

Local

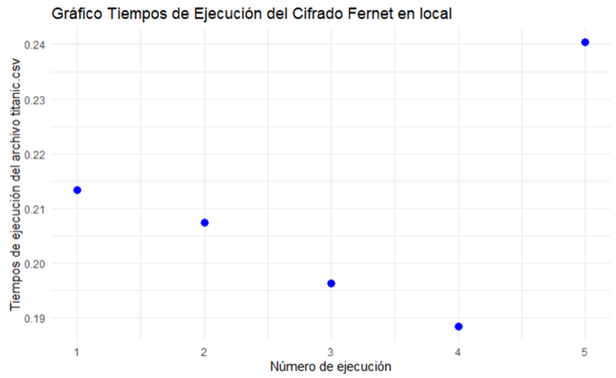

Figure 1. Tiempos de ejecución en local.

Cloud

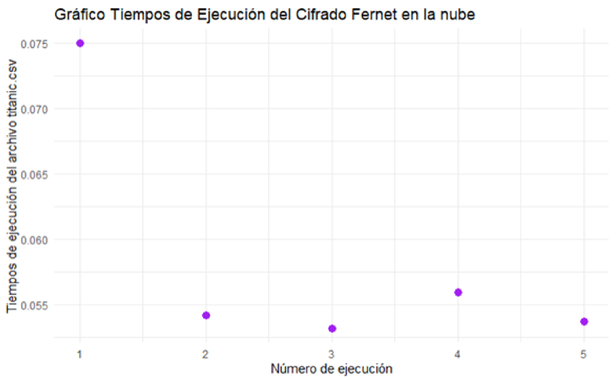

Figure 2. Tiempos de ejecución en la nube .

Conclusiones

A raíz de los resultados generados se llegó a las siguientes conclusiones:

- No influyo de manera significativa el entorno en el que se usaran los distintos algoritmos de cifrado en cuanto a tamaño de los archivos se refiere, puesto que los dos archivos variaron su tamaño en igual medida y valor en ambos entornos de ejecución (Tanto cloud como local).
- La variación mas notoria se vio reflejada en cuanto a tiempo de cifrado se refiere, esto ya que en el ambiente de la maquina virtual AWS los algoritmos tuvieron un performance notablemente mayor al obtenido en el ambiente local, tomándole menor tiempo a la máquina virtual el correr estos algoritmos. Esto se debe a que estas máquinas están optimizadas para el uso único y especifico de cómputo, mientras que la maquina local, aunque tiene más recursos, se encuentra ejecutando muchos más procesos en paralelo.
- Se evidencia que algoritmo Cesar es notablemente mas veloz que el algoritmo Fernet, sin embargo esto tiene que ver de igual forma con la fortaleza de cifrado de cada uno de los algoritmos (apoyados en el tamaño del archivo encriptado, el cual aumenta en gran medida con el algoritmo Fernet).
- En el caso del algoritmo Fernet, al ser un método mucho más robusto que el César, los archivos que usamos aumentan considerablemente en tamaño cuando se ejecuta el cifrado. Se hicieron varias pruebas con diferentes archivos .csv y se encontró que el encriptador agrega hasta un 33.3% más al tamaño del archivo, y en la computadora local, al momento de la ejecución de un archivo de 190 mb; se agotó la memoria RAM al generar el nuevo archivo encriptado. Por lo tanto, Es esencial tener en cuenta esto al emplear este método en una instancia en la nube, porque podría exceder los límites de los recursos, generando costos extras.

[1] Luis M. Vaquero1, Luis Rodero-Merino, Juan Caceres, Maik Lindner2 "A Break in the Clouds: Towards a Cloud Definition", ACM SIGCOMM Computer Communication Review, Vol. 39, No.1, 2009

[2] P. Mell y T. Grance, 'Cloud computing definition," NIST June 2009 http://csrc.nist.gov/groups/SNS/c1oud-computing/index.html

[3] "Fernet (symmetric encryption) — Cryptography 42.0.0.dev1 documentation". Welcome to pyca/cryptography — Cryptography 42.0.0.dev1 documentation. Accedido el 29 de noviembre de 2023. [En línea]. Disponible: https://cryptography.io/en/latest/fernet/cryptography.fernet.Fernet