

CHAPTER 5

ANALYSIS OF SECURITY ALGORITHMS FOR CLOUD COMPUTING

5.1 ABSTRACT

With growing awareness and concerns regarding data security for Cloud services, there is growing need to implement encryption practices for securing authentication access, user sessions, system applications and most importantly data in motion over unsecure Internet. Cloud Providers are focusing on ensuring end user data as secure as possible and having low priority for Cloud performance due to inconsistent selection of algorithms for encryption and encoding. This chapter compares the Cryptographic algorithms with emphasis on Symmetric algorithms for Cloud based applications and network services that requires securing data, session and links.

5.2 ENCRYPTION CONFIGURATION FOR CLOUD SECURITY

By selecting the right cryptographic scheme to use on devices and servers, data security is achieved without losing out on Cloud performance or availability issues. The below configuration is proposed by the author for ensuring secure algorithms in cloud devices.

- WAN Routers need to have IKE enabled for Crypto ISAKMP key exchange, anti-reply or Certification Authority which is shown below for 128-bit AES encryption, pre-shared key authentication

```
crypto isakmp policy 10  
encryption aes  
authentication pre-share  
group 19
```

- Site to site VPN devices encapsulate security payload (ESP) using 256-bit AES encryption and SHA 256 authentication when sending data in VPN tunnel mode using 3DES or RC4 algorithms as

```
crypto ipsec transform tier1-tunnel-transform-set esp-aes 256 esp-  
sha256-hmac1
```

- Network Switches should be required to use MD5 for encrypting user password as secret or use of Secure Copy Protocol (SCP) during device configuration or device IOS image copy via SSH using RSA

interface Serial0

ip address 192.168.4.2 255.255.255.0

ip ospf message-digest-key 1 md5 c23\$c0#1

- Servers need to imbibe Federal Information Processing Standard (FIPS 140), which is a strong cipher suite to be implemented and involves use of RSA, 3DES and SHA-1 for Data Loss Prevention (DLP) Bit Locker for file level data encryption which requires setting up of encryption and OS recovery keys, enabling SQL Data Encryption using SQL DB Transparent Data Encryption (TDE).

5.3 PERFORMANCE ANALYSIS

The author setup cloud based application environment and infrastructure designed to receive data over unsecure Internet from the user by using an application developed to encrypt, decrypt and then send the data to the cloud application. The below infrastructure illustrates the setup required for this configuration:

- Connectivity: 1Mbps WAN circuit link connected to a public Cloud server provider
- Cloud Simulation: Hosted Web application server on the IaaS systems
- Programming language environment – Java and .NET
- Server: Intel Core i5-3230M CPU @ 2.66GHz, 64 bit, 8GB memory.
- Windows Server 2008 running IIS web services on VMware Virtual machine

The author compared Symmetric encryption and encoding algorithms using data size and time involved to determine the selection for the correct algorithms based on the following parameters.

- File Size indicates file of different size to be taken
- Encryption Computation Time taken to produce cipher text from plain text
- Encoding Computation Time taken by encoding algorithm to produce a hash code

Performance metrics are collected based on the following:

- Encryption & Decryption Time is calculated as the time required for encryption which involves converting the plain text payload file into cipher text. Encryption time is considered to find the through put which indicated the computation cost i.e. the encryption speed. The decryption time is calculated for time required for converting the cipher text back into the plain text.
- CPU Processing Time is determined as the time CPU is committed for the process and reflects the CPU load during the encryption process. The CPU Clock Cycle and Battery power are the energy consumed during encryption and decryption process.
- Size of payload tested is actual size of test file being used for the experimental work.

The application is designed for accepting input as a text file taking File upload (path as E:\passfile.txt), Choosing encoding algorithm (DES, 3DES, AES), Hash, Key size and Mode (Encrypt or Decrypt) as shown in Figure 5.1.

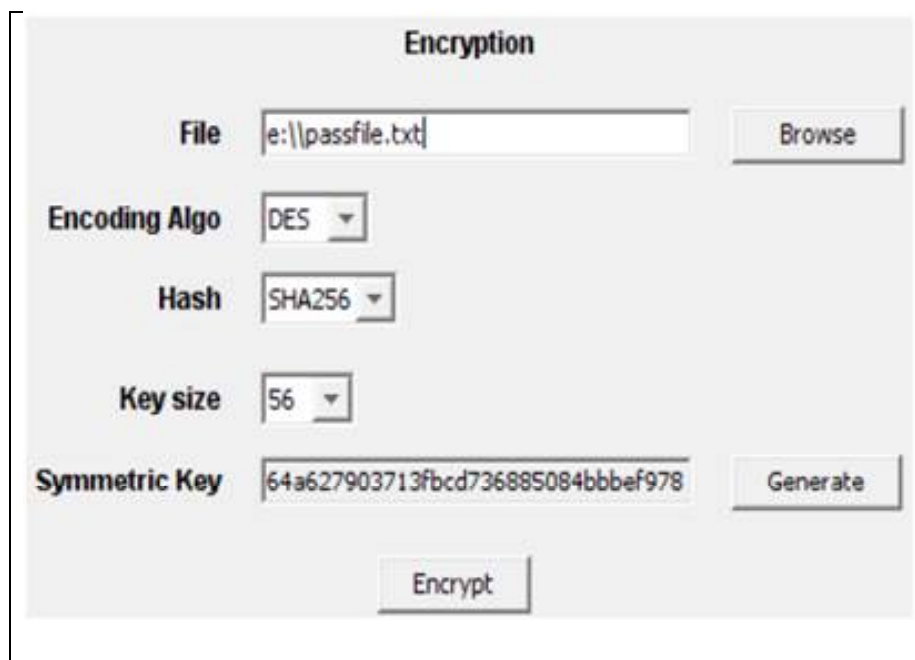


Figure 5.1: Encrypting text file to send to Cloud

The encryption of the data (text file) is considered to determine the time required for reading the file, encrypting the file, converting into the encrypted data, sending the encrypted data to a Cloud location and finally receiving the confirmation. Data from experimental work on Symmetric algorithms is represented by using varied file sizes as input and recording the computation cost for those algorithms.

Figure 5.2 below presents the computational cost for performing encryption by DES, 3DES and ASE algorithms against increasing payload.

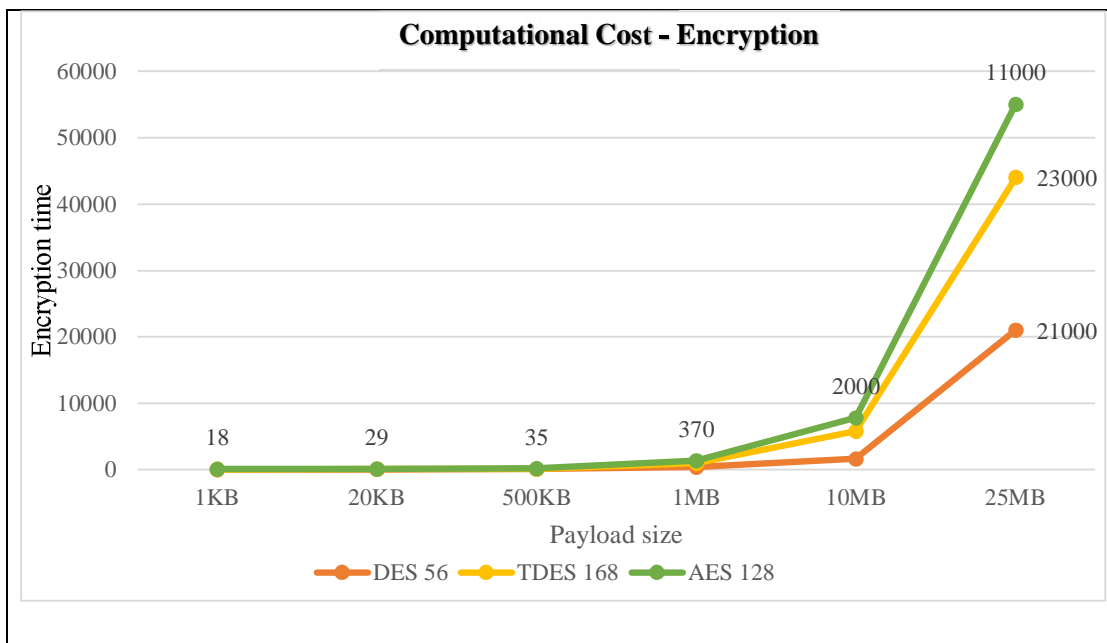


Figure 5.2: Computational Cost for Encryption

During the decryption process, algorithms check data integrity on Cloud and the computation cost data is obtained for algorithms by varying the size of payload as shown in Figure 5.3 below.

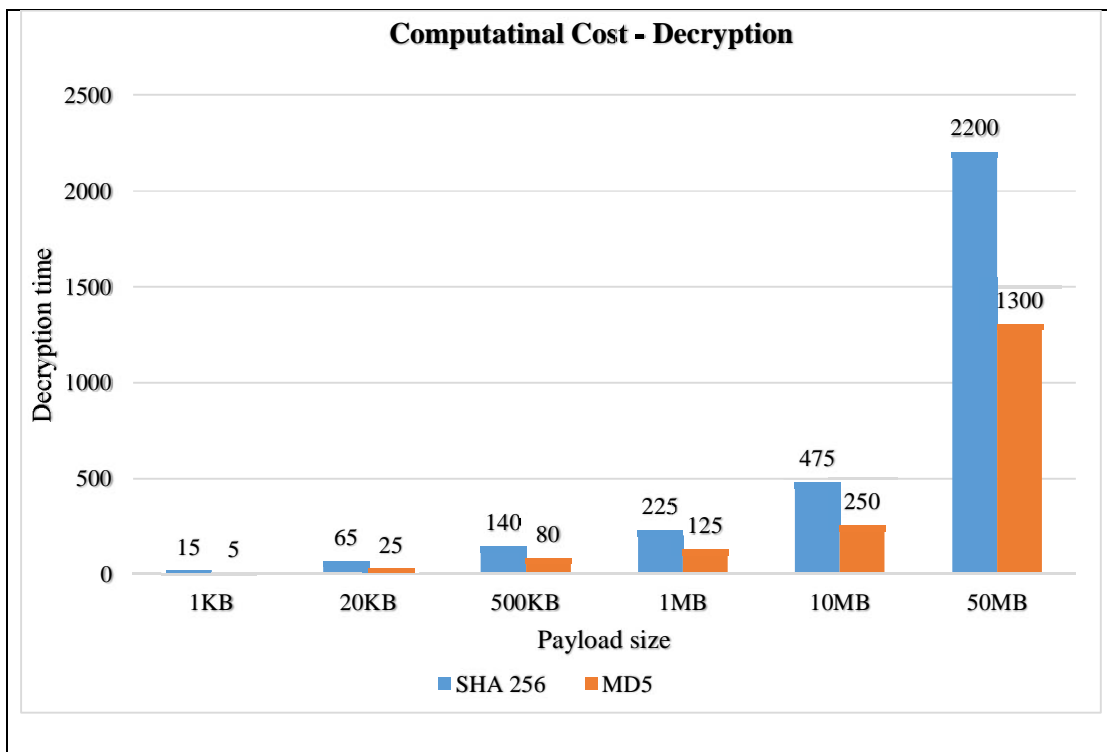


Figure 5.3: Computational Cost for Decryption

Encoding algorithms checks for data integrity for end user data and the computation cost data is obtained for different algorithms by varying the size of payload as shown in Figure 5.4 below.

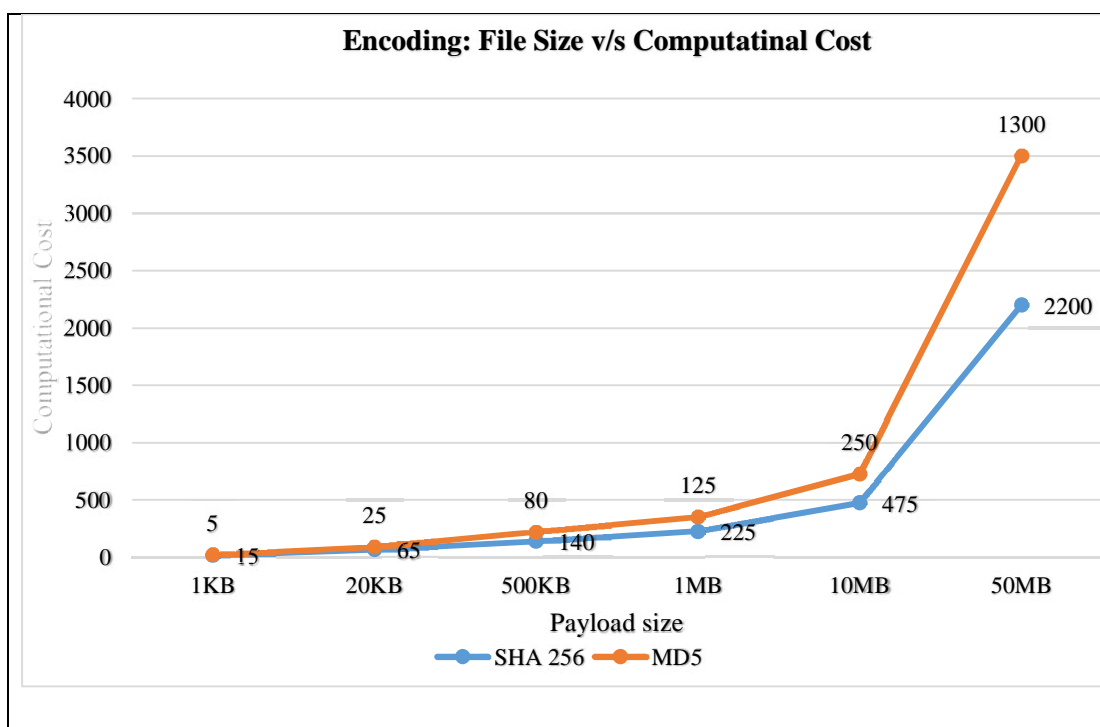


Figure 5.4: Encoding: File Size v/s Computing Cost

Observations from the work performed are presented as follows.

- Data Security for Cloud based applications can be increased by using RSA and AES Encryption algorithms. When using keys as 1024 bit RSA and 128 bit AES, determining the private key is not possible even if the attacker has the public keys generated
- After the end user logs in to the Cloud web portal, accesses the applications but does not log out and in fact just leaves the session idle, then in this case if an attacker breaks in to the user system attempting to download and access the data from the user system, then the attacker would be required to enter the private key. In case the attacker is successful in breaking in to the user system and even able to somehow guess the private key, then the encrypted data can be download.
- The attacker might be successful in getting the encrypted data but still accessing the original data might still not be possible.

CHAPTER SUMMARY

With Cloud computing emerging as a new in thing in technology industry, public and private enterprise and corporate organizations are either using the Cloud services or in process of moving there but face security, privacy and data theft issues. In this chapter, Symmetric algorithms are analyzed and AES is found to be a good candidate for key encryption while MD5 is faster when encoding. A combination of these algorithms can be implemented as a future research for securing end user data when using Cloud based applications.

The next chapter illustrates the proposed secure design in form of a three tier architecture to mitigate DDoS attacks. The three tier architecture is designed, implemented and DDoS attacks are performed on the environment. Similar attacks are performed on a single tier data center simulating a standard Cloud architecture. The two architectures are compared and their results are presented in subsequent chapters.