ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 8, Special Issue 1, August 2021

A Comparison of Data Encryption Algorithm's Performance in Cloud

Bindu Madavi K P
Dept. Computer Science and Engineering
Dayananda Sagar University, Bangalore
bindumadavi-cse@dsu.edu.in

Abstract—Cloud services are being used by businesses of all sizes, regions, and industries. This is because it has seen the fastest adoption into the mainstream than any other technology in the domain. Cyber-attacks are increasingly common, especially in education, finance, healthcare, and the public sector. The shift from on-premises data storage to cloud storage, which is connected by wired and wireless technologies, is the reason for the growth. While cloud platforms make it easier to store large databases of customer, employee, financial, and sales information, hackers can exploit loopholes in cloud computing to gain unauthorized access by spoofing it. This article will cover various encryption methods. The main objective is to analyse and compare the performance of different cryptographic algorithms to improve data security in cloud computing.

Index Terms—Cloud Computing, Cryptographic algorithms, Encryption, Performance

I. INTRODUCTION

Data security has become increasingly important in today's world. Every company has large amounts of data in its database that must be safeguarded. If this information is hacked in any way, the company will be severely harmed. Data is perhaps an organization's most important asset. Regardless of legal or regulatory constraints, it is in a company's best interests to keep its data secure. In their personal lives, everyone requires data security. Personal information is stored online and stored on servers with an uninterrupted connection to the cloud or the web. Cryptography plays a key role in data protection. In our daily lives, the use of cryptography is ubiquitous. Cryptography is the science and art of changing messages so that they are secure and resistant to unauthorized access[4][5]. It is a crucial component in the development of information systems. It is concerned with the study of mathematical techniques about issues of data security such as confidentiality, data integrity, and data authentication[1][2]. Various mathematical processes are used to secure cryptographic methods in a wide range of applications[3].

In cryptographic terminology, plain text is data that can be read and understood without too much action. Encryption is a method of hiding plain text to hide its essence. Plain text creates an unreadable pad called an encryption cipher. The process of getting plaintext from a cipher is called decryption. Figure 1 shows the encryption and decryption process. The system or product that provides encryption and decryption is called a cryptosystem [1][6]. In the field of information security, many encryption methods are widely available and used. The asymmetry and symmetry encryption algorithms are of two types. Only one key must encrypt and decrypt data using symmetric-key cryptography, also known as secret-key cryptography. Asymmetric keys use two keys: one private and one public. Encryption is done using the public key, and decryption is done using the private key. Cryptography plays an important role in solving these problems. Strong and well-established

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 8, Special Issue 1, August 2021

data encryption has benefited from online and incredibly valuable assets or properties.

II. RELATED WORK

In general, there are three sorts of cryptographic techniques Symmetric Encryption, Asymmetric Encryption, and Hashing function. Figure 2 shows the classification of cryptography. With symmetric encryption, a key is used by both the sender and the recipient. The sender encrypts the plaintext and sends the ciphertext to the recipient using this key. On the other hand, the recipient uses the same key to decrypt the message and receive the plaintext. Different types of symmetric key encryption: AES, DES RC2, IDEA, Blowfish, Stream cipher. In asymmetric cryptography, there are two associated keys (public and private). The public key can be transferred freely, but the private key must be kept secret. The public key is used for encryption, and the private key is used for decryption. Some of the types of asymmetric key cryptography are RSA, DSA, PKC, Elliptic curve techniques. Keys are not used in the Hash function. Plain text is hashed using a fixed-length hash value, which prevents the contents of plain text from being retrieved. Many operating systems also use hashing algorithms to protect passwords.

A. Advanced Encryption Standard(AES)

Joan Daemen and Vincent Reiman created the AES algorithm, a block cipher of symmetric keys, in 1998 [9]. AES is a symmetric-key algorithm that encrypts and decrypts, indicating that the sender and recipient use the same key. The length of the AES data block is 128 bits. The key size is 128, 192 or 256 bits [7]. This is an iterative algorithm, and each move is called an iteration. When the key length is 128, 192, or 256 bits, the total number of turns is NR, 10,12 or 14 [8]. AES uses several transformations to ensure security. Each AES cycle, except the last one, uses all four modifications for permutation , substitutions, mixing, and key addition [7]. Each cycle is a set of four basic changes that use encryption. The decryption engine uses the reverse order of the steps specified in the encryption method. The basic structure of encryption and decryption in the AES method is shown in Figure 3. Subbyte, shift row, mix column and add round key are the four basic transformations performed at each pass [10].

1. SubByte: A non-linear replacement byte that uses a replacement table to work with each status byte individually.
2. ShiftRow: Numbers are shifted cyclically from individual bytes.
3. MixColumn: column with multiple columns
4. AddRoundKey: Using the basic XOR method, add a round key to the report.

B. Data Encryption Standard(DES)

DES is a block cipher with a key size of 56 bits and a block size of 64 bits. IBM developed DES in 1972 as a data encryption method. The US government adopted it as the standard encryption algorithm. It started with a 64bit key, but the NSA has limited its use to 56-bit keys, so DES removes 8 bits from the 64-bit key and then uses the 56-bit compressed key derived from the 64-bit key cryptography. 64-bit block data [9] DES is a 16-pivot substitution and exchange algorithm. The data and key bits are moved, exchanged, XORed, and sent through 8 s-boxes, the set of lookup tables required by the DES algorithm, at each cycle. Decryption is essentially the same procedure as encryption, but the reverse is true [7].

As shown in Figure 4, DES is a block cipher. DES creates a 64-bit ciphertext from a 64-bit plaintext; At a decryption site, DES creates a 64-bit plaintext block from a 64-bit ciphertext. The same 56-bit encryption key is used for encryption and decryption.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 8, Special Issue 1, August 2021

The encryption procedure consists of sixteen Feistel turns and two permutations (P-boxes), which we call beginning and end permutations. Each move uses a separate 48-bit key derived from the encryption key using a predefined technique. Parts of the DES encryption are shown in Figure 5 at the encryption site [11].

C. Triple Data Encryption (3DES)

3DES is a block cipher. 3DES was first released in 1998 and gets its name because it encrypts, decrypts, and encrypts each data block three times using DES encryption[9]. Figure 6 shows 3DES showing encryption and decryption. Encrypt the data. Three times with three 56bit keys. This is a less risky version of DES. Start with DES and create a block cipher technique using the combined block method. 3DES is more secure than the original DES algorithm[12].

Here is the procedure for encryption-decryption:

Use a DES with the K1 key to encrypt blocks of text. Decrypt the result of step 1 with K2 using a single DES. Finally, encrypt the result of step 2 with K3 using a DES. The ciphertext is the result of step 3. The reverse process of decrypting the ciphertext is called decryption. K3 is used for decryption, then K2 is used for encryption, and finally, K1 is used for decryption.

D. Base64

Base64 encoding converts binary data into a text format that can be safely passed in contexts that only support text. The original binary data is split into 3-byte Base64-encoded tokens. Since the byte is eight bits long, Base64 only needs 24 bits. The ASCII standard is then used to convert these three bytes into four printable characters. The first step is to divide the three bytes of binary data (24 bits) into four six-bit values. Since ASCII requires seven bits, Base64 uses only six bits (26 = 64 equivalent characters) to ensure that the encoded data is readable and that none of the special ASCII characters are used. Base64 is the name of the algorithm, which derives from the use of these 64 ASCII characters. The numbers 09, alphabets, 26 lowercase, and 26 uppercase character, rs, and two additional characters ”+” and ”/” make up the ASCII characters used for Base64.

III. RESULTS AND DISCUSSION:

This section discusses the results of the scoring parameters. The algorithms are implemented in Java using the Eclipse IDE. Java encryption and security implemented. Encryption, decryption, key generation, key management infrastructure, authentication, and authorization are some of the security features provided by the java encryption and security packages. Table 1 and Table 2 shows the time it takes to encrypt and decrypt the same text with different encryption algorithms. Table 3 shows the comparison among AES, DES,3DES, and base64 algorithms. Figure 7 shows that AES took as little time as possible to encrypt three different encryption methods with input sizes of 5KB, 10KB, 20KB, and 50KB, respectively. The base64 algorithm, on the other hand, took longer, followed by DES and 3DES. For 5KB, 10KB, 20KB, and 50KB input data encryption, this method requires 39ms, 46ms, 61ms, and 114ms, respectively. Figure 8 compares the average time it takes to decrypt data of different sizes for four encryption methods (KB). It shows that DES takes the shortest possible time to decrypt data with input sizes of 5KB, 10KB, 20KB, and 50KB. Base64, on the other hand, took longer to decode the data with average decryption times of 13ms, 13ms, 14ms, and 26ms, sorted by input sizes of 5KB, 10KB, 20KB,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 8, Special Issue 1, August 2021

and 50 KB. Also, 3DES consumes most of the time after the Base64 algorithm.

IV. CONCLUSION

Using encryption to protect data by regulating access to such data is a technique that has been around for a long time, and, with the increasing use of information technology in every element of our human activity, it is becoming increasingly important. The experimental results of encryption methods are displayed, demonstrating that all techniques employ the same text files for testing. During the analysis, it was found that the time it takes to encrypt and decrypt is longer in base64. Compared to other algorithms, AES takes less time to encrypt and decrypt. AES is the best algorithm for use if cryptographic strength is a critical consideration in the application.

REFERENCES

[1] Panda, M. (2016, October). Performance analysis of encryption al- algorithms for security. In 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES) (pp. 278-284). IEEE.

[2] Jeeva, A. L., Palanisamy, D. V., Kanagaram, K. (2012). Comparative analysis of performance efficiency and security measures of some encryption algorithms. International Journal of Engineering Research and Applications (IJERA), 2(3), 3033-3037.

[3] Mushtaq, M. F., Jamel, S., Disina, A. H., Pindar, Z. A., Shakir, N. S. A., Deris, M. M. (2017). A survey on the cryptographic encryption algorithms. International Journal of Advanced Computer Science and Applications, 8(11), 333-344.

[4]Genc¸o g˘lu, M. T. (2019). Importance of Cryptography in Information Security. IOSR J. Comput. Eng, 21(1), 65-68.

[5] Hossain, M. A., Hossain, M. B., Uddin, M. S., Imtiaz, S. M. (2016). Performance analysis of different cryptography algorithms. International Journal of Advanced Research in Computer Science and Software Engineering, 6(3).

[6].Panda, M., Nag, A. (2015, May). Plain text encryption using AES, DES, and SALSA20 by Java-based bouncy castle API on Windows and Linux. In 2015 Second International Conference on Advances in mode for high-security applications." In Second International Conference on Current Trends In Engineering and Technology-ICCTET 2014, pp. 499-502. IEEE, 2014.

[7] Seth, S. M., Mishra, R. (2011). Comparative analysis of encryption algorithms for data communication1.

[8] Vaidehi, M., and B. Justus Rabi. "Design and analysis of AES-CBC mode for high-security applications." In Second International Conference on Current Trends In Engineering and Technology-ICCTET 2014, pp. 499-50.

[9] Awotunde, J. B., Ameen, A. O., Oladipo, I. D., Tomori, A. R., Abdul raheem, M. (2016). Evaluation of four encryption algorithms for viability, reliability, and performance estimation. Nigerian Journal of Technological Development, 13(2), 74-82.

[10] Naraei, P., Amiri, I. S., Saberi, I. (2014). Optimizing IEEE 802.11 i resource and security essentials: for mobile and stationary devices. Syngress

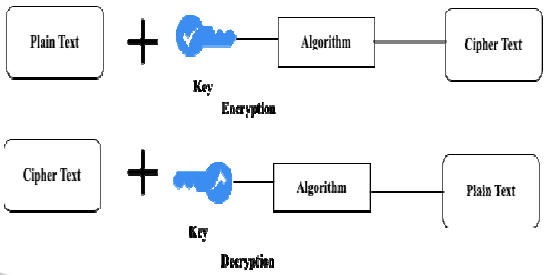
[11] D.S.M.-S.D.C.Y. (2015). Hands-on Experience in Security. Academic.Csuohio.Edu. https://academic.csuohio.edu/yuc/security/.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 8, Special Issue 1, August 2021

[12]Data Encryption Standard-Tutorialspoint. (2007). https://www.tutorialspoint.com/cryptography/dataencryptionstandard.htm.

Fig. 1. Encryption and Decryption.



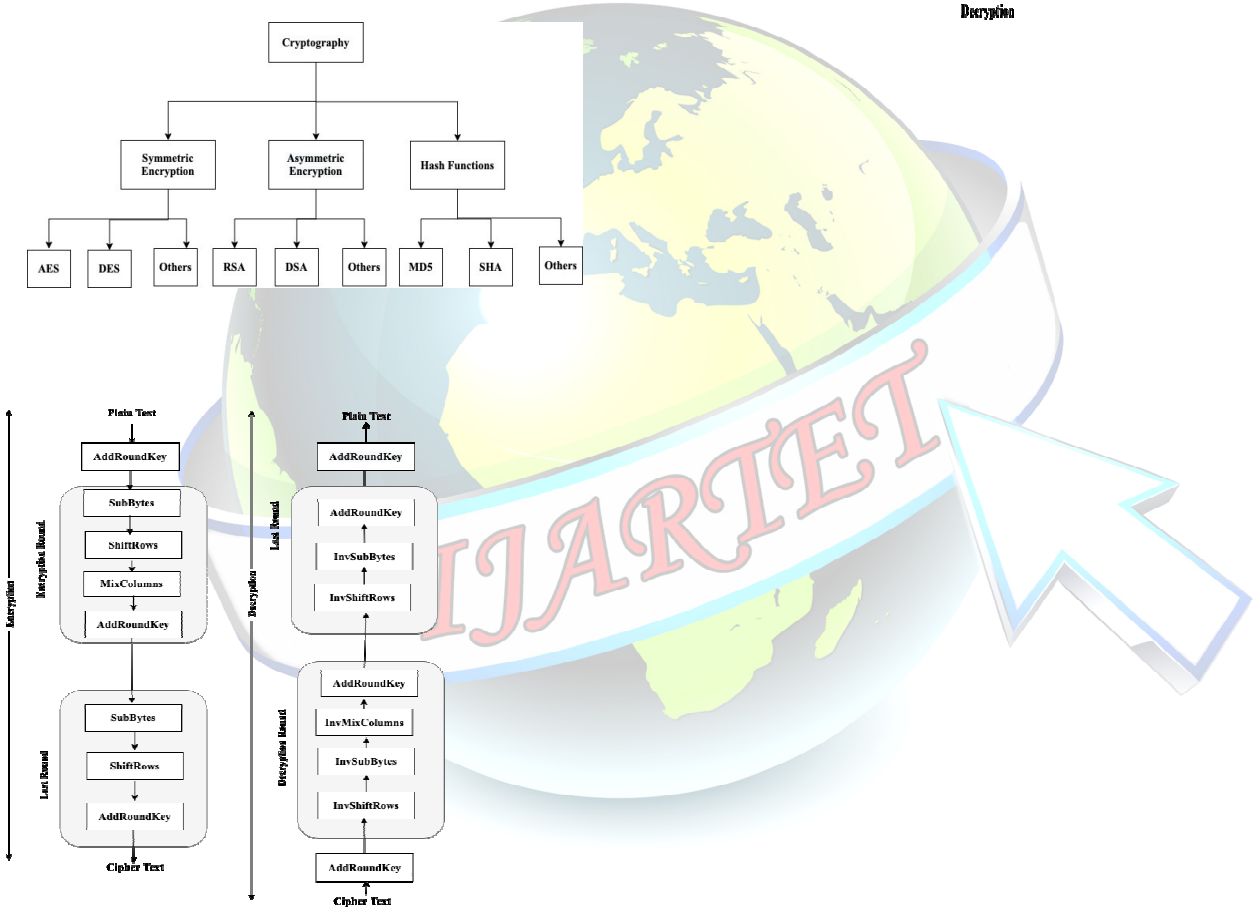
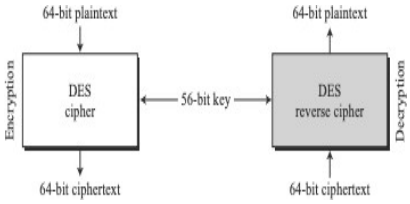


Fig. 2. Classification of Cryptography[6].

Fig. 3. AES Encryption and Decryption.



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 8, Special Issue 1, August 2021

Fig. 4. Encryption and decryption with DES.

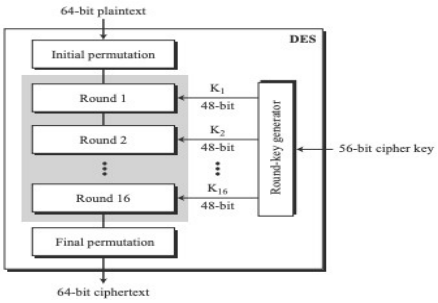


Fig. 5. General Structure of DES.

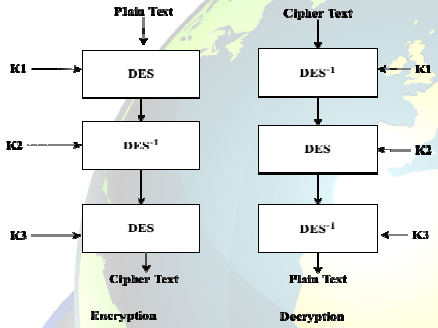


Fig. 6. 3DES encryption and decryption.

TABLE I
ENCRYPTION TIME FOR DIFFERENT FILE SIZE

Algorithms	5KB	10KB	20KB	50KB
AES	4milliseconds	7milliseconds	11milliseconds	18milliseconds
BASE64	39milliseconds	46milliseconds	61milliseconds	114milliseconds
DES	5milliseconds	9milliseconds	12milliseconds	17milliseconds
3DES	7milliseconds	16milliseconds	22milliseconds	31milliseconds

TABLE II
DECRYPTION TIME FOR DIFFERENT FILE SIZE

Algorithms	5KB	10KB	20KB	50KB
AES	1milliseconds	2milliseconds	6milliseconds	12milliseconds

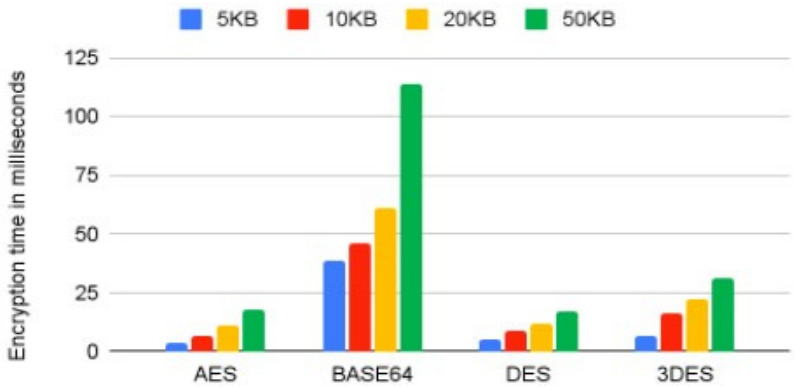
ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 8, Special Issue 1, August 2021

BASE64	13milliseconds	13milliseconds	14milliseconds	26milliseconds
DES	1milliseconds	2milliseconds	3milliseconds	6milliseconds
3DES	1milliseconds	4milliseconds	7milliseconds	16milliseconds

TABLE III
COMPARISON OF EXECUTION TIME AMONG AES,BASE64,DES,3DES

Encryption Algorithm	Plain text	Cipher Text	Encryption time	Decryption time	Memory used in bytes
AES	hi, to welcome my git area!	acd7fddda5793cef7ba666c21ebc38b82919baeabbcabb4b7c2a7c004a817926	3 milli seconds	0 milli seconds	1224096
base64	hi, to welcome my git area!	aGksIHdlbGNvbWUgdG8gbXkgZ2l0IGFyZWEh	35 milli seconds	5 milli seconds	605200
3DES	hi, to welcome my git area!	8f54f86cf8f3fa2fc6942c7466ea39e6b6e9e3ad118bbf64d8a1910def2ebcbe	3 milli seconds	0 milli seconds	1179216
DES	hi, to welcome my git area!	f9c2e3f6443d2ebb4cea492b0df87e105901ab75885f158d5cfad57f6a5c5fd9	3 milli seconds	0 milli seconds	1215488



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 8, Special Issue 1, August 2021

Fig. 7. Average Encryption Time.

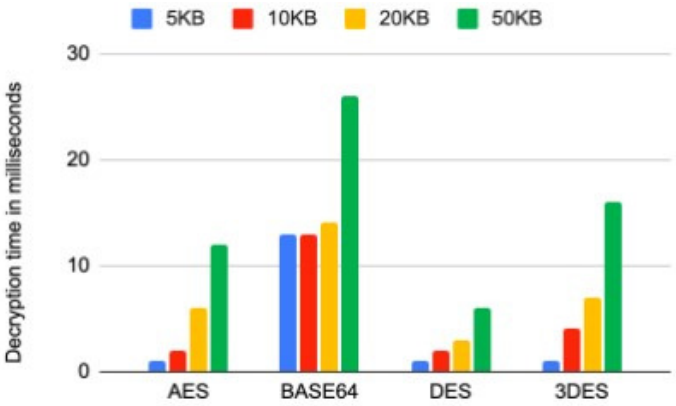


Fig.8. Average Decryption Time