ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 2, Issue 10, October 2013

Evaluation and Comparison of Symmetric key algorithms

Gurpreet Kaur, Manish Mahajan

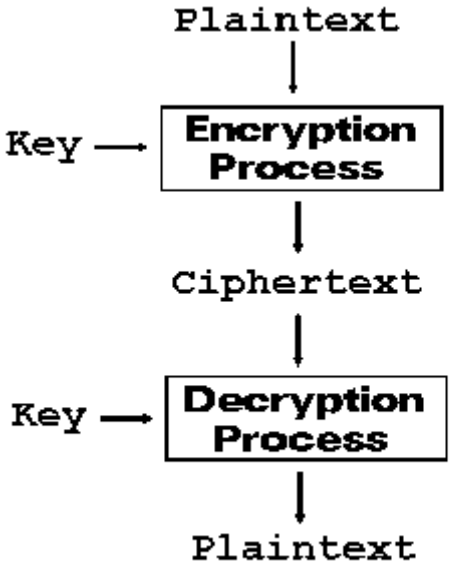
***Abstract*— Cryptography is an art and science. It plays major role in information and security sector. Personal privacy is of important in the every sector of the world. Best way to safeguard the personal information is the use of cryptography. There are two basic cryptographic algorithms Symmetric key algorithms and Asymmetric key algorithms. Symmetric key algorithms are said to be as the most commonly used. Symmetric key, the speed to encrypt data is fast.**

This paper presents the comparison between the symmetric key algorithms. The algorithms are compared on local system as well as on the cloud network.

***Index Terms*— Symmetric key algorithms, AES, DES, DESede , BLOWFISH.**

I. INTRODUCTION

The security in computer systems can be increased by is encrypting the data. The original data is called the plaintext. The process of converting a plain text message to its ciphertext form is called enciphering . In its cipher form, a message cannot be read by anyone but the intended receiver. Reversing that process (i.e., ciphertext form to plain text message) is deciphering. Enciphering and deciphering are more commonly referred to as encryption and decryption.

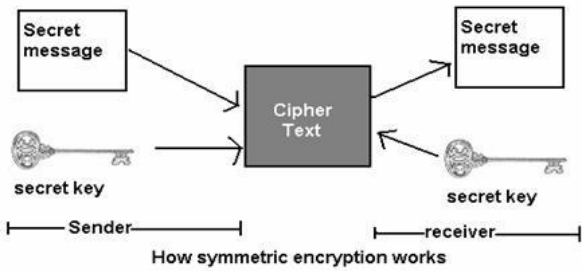


This paper presents the comparison between the Symmetric Key algorithms on speed-up ratio and Mean time. Section II is the Cryptographic techniques ,Section III presents the algorithms used, Section IV states the Parameter Analyzed, section v is Methodology used, section V consists of results and last section VI is Conclusion.

II. CRYPTOGRAPHIC TECNIQUES

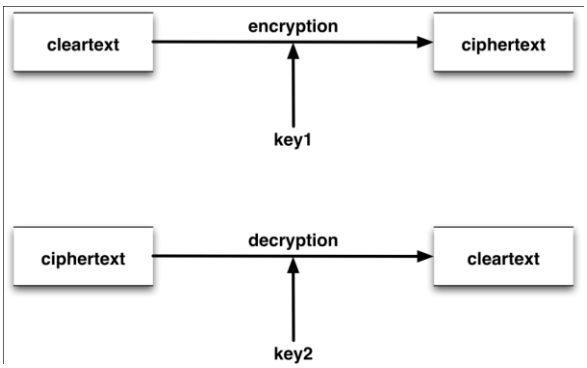
There are mainly two types of cryptographic techniques:

1) **Symmetric key algorithm**: Symmetric algorithms are also called as secrete key algorithms. In secrete key algorithms both parties (Sender, Receiver) will use the same key to encrypt or decrypt the data. Example for symmetric key algorithms is DES, AES, Triple DES, and Blowfish.[7]



How symmetric encryption works

2) **Asymmetric key algorithm**: - Asymmetric key algorithms also called public key algorithms. In public key algorithm both parties (sender and receiver) having their own different keys. In this, the sender will encrypt the plain text with the public key of receiver and receiver will decrypt the cipher text with private key. The private key is kept confidential.[7]



All Rights Reserved © 2013 IJSETR

III. ALGORITHMS USED:-

1) AES: In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively [2]

2) DES:- The DES (Data Encryption Standard) algorithm is the most widely used encryption algorithm in the world. For many years, and among many people, "secret code making" and DES have been synonymous meaning it operates on plaintext blocks of a given size (64-bits) and returns cipher text blocks of the same size.[2]

3) BLOWFISH:-Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. In structure it resembles CAST-128, which uses fixed S-boxes. The diagram to the left shows the action of Blowfish. Each line represents 32 bits. The algorithm keeps two subkey arrays: the 18-entry P-array and four 256-entry S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. One entry of the P-array is used every round, and after the final round, each half of the data block is XORed with one of the two remaining unused P-entries.

4) DESede:- Data is encrypted using the DES algorithm three separate times. It is first encrypted using the first subkey, then decrypted with the second subkey, and encrypted with the third subkey.[8]

IV. PERFARMANCE ANALYSIS PARAMETERS:

By using algorithms, the speed-up ratio and the mean processing time for different inputs are calculated.

4.1. Speed-Up ratio is defined as the difference between the mean processing time of single system and the cloud network. Speed-up ratio will provide tell us how quickly the data have been encrypted

4.2. Mean processing time is the difference between the starting time taken to encrypt the data and the ending time. It is the difference between the time taken to encrypt the data. As the size of input increases the time taken to encrypt the data will increase and with the increase in time speed-up ratio decreases.

V. METHODOLOGY

To compare the symmetric key algorithms, the users implement their application for deploying them on the cloud. Cloud software environment provider supplies the developers with programming-level-environment with well defined set of API's. The service commonly provided by this layer is referred to as Platform as a Service (PaaS). One example is Google's App Engine, it provides a runtime environment and set of API's [2].

For interaction with Google's cloud runtime, applications are run on "sandboxed" environment. As the request increases for an application, App engine offers automatic scaling for web application. Google App is free up to certain level of consumed resources, charges applied for the additional storage and bandwidth [2]. Experimental evaluation is done on eclipse-SDK and Google App engine. The evaluation is done for different input sizes: 10KB, 13KB, 39 KB, and 56 KB.

For the data security, we have used four encryption algorithms: AES, DES, BLOWFISH and DESede. Using java on eclipse the algorithms are run on local as well as on Google app engine.

VI. RESULTS

Comparing Speed-up ratio and Mean time are used to select the highest security algorithm. Four encryption algorithms are being used namely AES, DES, BLOWFISH and DESede.

Table 1: Comparison of Mean processing time of the algorithms on local system as well as on cloud network

Input	AES	AES CLOUD	DES	DES CLOUD	BLOWFISH	BLOWFISH CLOUD	DESede	DESede CLOUD
10 kb	11.5	1.5	7.5	2	4	2	12	4.5
13 kb	14.7	2	10	2.5	4.7	2	15.5	5.25
39 kb	21	3	31.5	6.5	8.25	2.75	47.25	10.25
56 kb	24.5	3.75	50.25	9.25	15.7	3	70.5	14.5

Mean processing time is calculated in milliseconds.

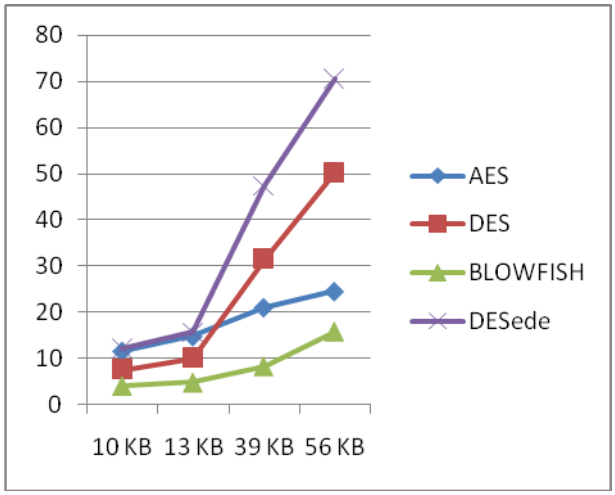


Fig: 3: Comparision of local system mean time algorithms with different inputs.

All Rights Reserved © 2013 IJSETR

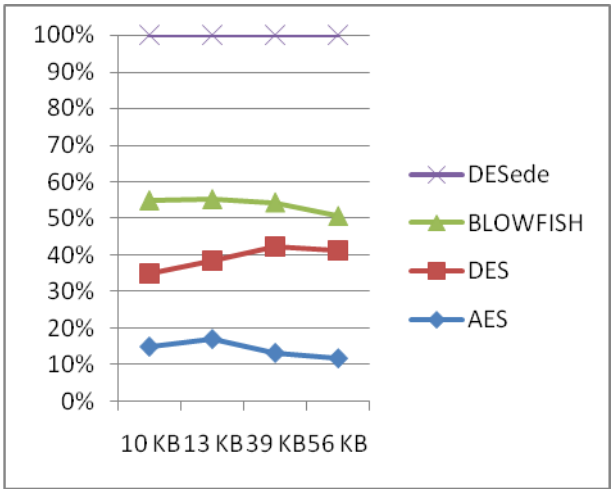


Fig 4: comparison of Cloud mean time for algorithms with different input sizes.

Table 2:Speed-up ratio of the algorithms for different input sizes

INPUT	AES	DES	BLOWFISH	DESede
10 KB	7.6	3.62	2	2.6
13 KB	7.2	4	2.3	2.9
39 KB	7	4.8	3	4.6
56 KB	6.6	5.43	5.25	4.8

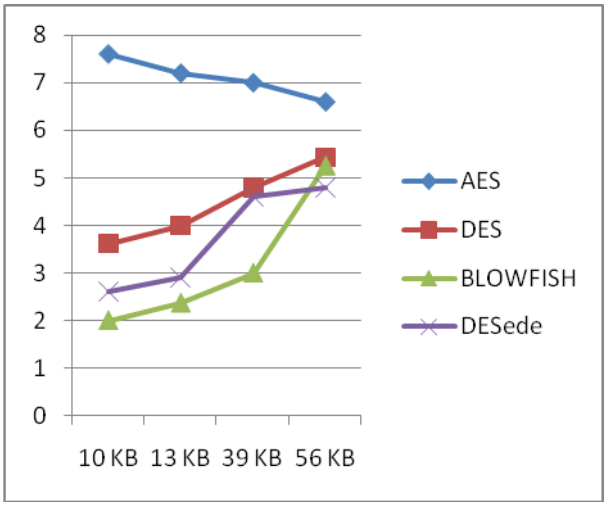


Fig 5: Comparison of speed-up ratio of the algorithms for different inputs.

From the Tabular results, the following observations can be made, using eclipse run variable input sizes on local as well as on Google App engine. Among all the algorithms DESede-an symmetric encryption algorithm is average most time consuming and BLOWFISH is algorithm is the least time consuming.

AES-a symmetric encryption algorithm, the speed-up ratio falls sharply with the increase in input size.AES algorithm has the highest speed-up ratio and then is DES.

In AES algorithm the speed up ratio decreases with the increase in size. Whereas DES and BLOWFISH remains almost constant. There is a slight change in the speed-up ratio for DES and BLOWFISH.

VII. CONCLUSION

Cryptography is used to achieve Confidentiality, Authentication .In order to achieve these goals various cryptographic algorithms are developed by various people. From the above results, when you are interested in performance of algorithm, go for BLOWFISH, AES and DES.

For the security of data, go for the AES.

Finally for less time and more secure algorithm, AES algorithm is best.

REFERENCES

[1]Sherif El-etriby, Eman M. Mohamed, Hatem S. Abdul-kader" Modern Encryption Techniques for Cloud Computing Randomness and Performance Testing"in ICICT ,800-805 ,2012.Definition ", ACM SIGCOMM Computer Communication Review, Vol. 39, No. 1, 2009

[2] Priyanka Arora, Arun Singh, Himanshu Tyagi "Analysis of performance by using security algorithm on cloud network" in international conference on Emerging trends in engineering and management (ICETM2012), 23-24 June , 2012

[3] Priyanka Arora, Arun Singh, Himanshu Tyagi " Evaluation and Comparison of Security Issues on Cloud Computing Environment" in World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5, 179-183, 2012.

[4]http://en.wikipedia.org/wiki/Triple_DES, cited on Aug 21,2013

[5]Ayushi, "A Symmetric Key Cryptographic aalgorithm", International Journal of Computer Applications, 2010.

[6] B. Forouzan, "Cryptography and Network ecurity" 4th edition, Mc Graw Hill, Inc 2007.

[7]Kamini H. Solanki[1], Chandni R. Patel[2"] New Symmetric Key Cryptographic algorithm for Enhancing Security of Data "International Journal Of Research In Computer Engineering And Electronics. PAGE # 1 ISSN 2319-376X VOL :1 ISSUE :3 (DEC 2012) .

[8] http://www-01.ibm.com/support/docview.wss cited on 27 sep 2013.

***Gurpreet kaur**, Department of Information Technology, Chandigarh engineering Collge,Landran(Mohali)., Mohali, India,*

***Manish Mahajan**, Associate Professor, Department of Information Technology, Chandigarh engineering Collge,Landran(Mohali)., Mohali, India,*

All Rights Reserved © 2013 IJSETR