Available online at www.ijiere.com
International Journal of Innovative and Emerging Research in Engineering
e-ISSN: 2394 – 3343 p-ISSN: 2394 – 5494

Performance Analysis of AES, DES, RSA And AES-DES-RSA Hybrid Algorithm for Data Security

Prof.S.N.Ghosh [a] , Deepak T Biradar [b], Ganesh C Shinde[c] , Sarika D Bhojane[d] , Manojkumar R Shirapure[e]
[a] Assistant Professor, Computer Engineering & IT Department, College of Engineering Pune, Shivajinagar, Pune, India.
[b,c,d,e] Computer Engineering & IT Department, College of Engineering Pune, Shivajinagar, Pune, India.

ABSTRACT:
Network security typically based on authentication which might start with a simple username and a password. This is just 1-factor authentication (one username and one password), But generally 1-factor authentication does not serve the purpose of full security for sensitive data transmission .To send the data (generally more sensitive) we have to wrap the data using some algorithm(like AES or DES) and put over the network. Now a day due to high speed computers these algorithms are now vulnerable to attacks. In this project we propose the idea of using a combination of AES-DES-RSA and incorporating it in the Feistal structure. Being a hybrid of three powerful encryption techniques, the algorithm would be an efficient and reliable encryption standard. This project will contain the implementation and design of a of hybrid based AES-DES-RSA algorithm for the security purpose.
Data Encryption: Using Hybrid AES-DES algorithm Key Exchange Mechanism: Using RSA-1024.
Our Algorithm will mainly focus on following parameters:
1. Avalanche Effect
2. Encryption Time
3. CPU Usage
4. **Throughput**

Keywords: AES Algorithm, DES Algorithm, Feistel Structure, RSA algorithm, Hybrid Algorithm.

I. INTRODUCTION

In today's world data security has become a prime parameter with the changing scenario of the security constrains. Some of the algorithms given their best with time but become vulnerable with time as DES algorithm can be broken in 24 hours [5], so it has emerged some of the security constrains; though AES and RSA are not vulnerable right now but in future they can, so considering future scope of the data security we propose a hybrid algorithm of AES-DES-RSA for better security and performance of the algorithm.

II. AES

AES (Advanced Encryption Standard) is dependent on pattern, basic principle associated with substitution permutation system. AES carries a predetermined block size associated with 128 bit along with a essential size associated with 128, 192 or perhaps 256 little. AES functions on 4 X 4 matrix associated with bytes, mentioned as state. AES has four methods which are the following: shift rows, Mix column, substitute bytes, Add around sub-key.[2]

Encryption Process:

The process of encryption in AES uses special keys called round keys. These keys are applied with other operations like Sub Bytes, Shift Rows etc. on plaintext (original data) to get cipher text (encrypted data).Total six steps involved in the encryption process of AES, those are(assuming128 bit of plaintext).[2]

1. Derivation of Round Keys
2. Initialization of State array.
3. Add initial round key.
4. Perform rounds.
5. Perform Final round.
6. Get cipher text.

Round computation:

For the first nine rounds all four operations will be done and for last round the Mix Column operation is not performed.[2]

SubBytes Step:

Converting every byte into another byte is the main task of this step. There are 256 different values defined in AES for substitution. In 256-byte substitution table use every byte as an index to 256- byte substitution table and we get totally new bytes (state array). .[2]

ShiftRows Step:

The Shift Rows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively..[2]

Mix Columns Step:

In this step columns are processed instead of rows, each column is computed (Matrix Multiplication) to generate new column and old column is replaced by new one.[2]

Add Round Key:

In this last step of round, XOR operation take place between existing state array and round key. Output of this will replace state array.[2]

Limitations of AES:

1. AES algorithm need more processing time.
2. AES require more rounds of communication as compare to DES**.**
3.

III.DES

DES algorithm is widely used block cipher in the world because of its simplicity.DES consist of 64 bit block size and uses 56 bit key size.DES contains 16 rounds for processing and became a more secured algorithm. DES uses same procedure like feistel structure of cryptography.DES contains initial permutation block of 64 bit which is divided into two blocks of each 32 bits. These two blocks called as left(L) and right(R) part of the block. In DES algorithm permutation and substitution steps can be repeated by 16 times i.e. DES contains 16 rounds for processing, re-joining of left and right part can be done by applying inverse initial permutation.[3]

Encryption Process:

There are total six steps involved in the encryption process of DES.[3]

Steps:

1. Initial Permutation.
2. Divide into Two halves.
3. Right Half through feistel function f.
4. X-OR with left half.
5. Swapping.
6. Inverse IP at last step.

Fiestel function f in third step consist of four functions, those are Expansion, Key Mixing, Substitution, Permutation.[3]

Limitation of DES:

1) DES uses 56 bit key size which is too small that's why it is easy to break algorithm in 22hrs and 15 minutes from group of people or computers. 2) Using brute-force attack it is possible to break DES algorithm easily because system can secured with only 8 character passwords**.**

IV.RSA

RSA (Rivest-Shamir-Adleman) is public key encryption algorithm. Most of the countries uses network security provider for RSA algorithm. Now a day's RSA is widely use for secure data transmission and RSA contains public encryption key and decryption key is secret for secure data transmission.RSA mainly based on factoring of product of two prime numbers. These two prime numbers are kept secret and no one knows it without authorized user. If the public key is large then the message can decode only that someone with knowledge of prime number [4].

Key Generation [4]

step 1: take any two prime numbers say a and b.
step 2:Compute n such that n = a * b.
step 3:Compute totient of n, (n) (n) = (a - 1) * (b - 1)
step 4:Choose a value e s.t. 1 < e < (n) and e and (n) should be relatively prime.
step 5: Compute d such that, de = 1 (mod (n)).

Encryption [4]

Cipher text is calculated by
c = me (mod n), where m is plaintext.

Decryption [4]

Plaintext is calculated from cipher text by M = cd (mod n)

V. PROPOSED SYSTEM

Hybrid Algorithm

The design of hybrid Algorithm constructed using DES Feistel structure and AES properties in it. The complexity depends on the number of iterations as performed by feistel structure, as more number of rounds more complexity will be there in Hybrid Algorithm (case of DES number of round are 16).

Two equations on which Hybrid Algorithm rely are, Left1= f (Right0)..... (1) Right1=AES (f (Left0)) XOR f (Right0)..... (2)

User have to enter the plaintext in the multiple of 256, the plaintext is then divided into two equal parts of 128 bits each. Again these two parts are divided into four parts of 64 bits each. Using user input key these four parts are encrypted. We are using only one key for both encryption and decryption also. Means we are using the same key for AES as well as DES.192 bits of data is formed by DES encryption. f (Left0) is formed by clubbing two left parts similarly F(R0) is formed by clubbing two right parts. f (Left0) and f(Right0) are 384-bits each long. After getting Left0 and Right0 both are XOR with each other. Now this cipher-text from DES is given to AES Algorithm as plaintext and the cipher-text is again encrypted using key given already. Encrypted text length is now 704-bits long. Then Right0 is assigned to Left1 and the output of AES is given to right part i.e. Right1. 1088 bits of encrypted data is formed after clubbing Left1 and Right1 part. We follow the exact reverse procedure to get plaintext back.

VI. ARCHITECTURE OF PROPOSED SYSTEM

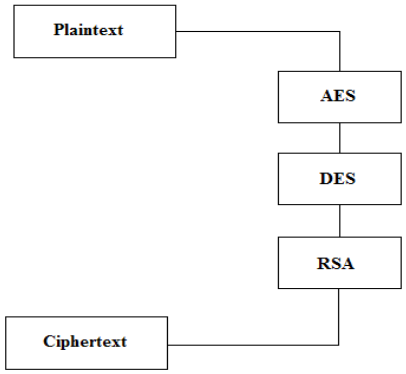

Fig 1: Hybrid encryption approach

VII. ANALYSYS OF HYBRID ALGORITHM

GUI for proposed system

The tool used by us for building GUI for the proposed system is NetBeans, having platform of JAVA language, here is the main frame for the same:

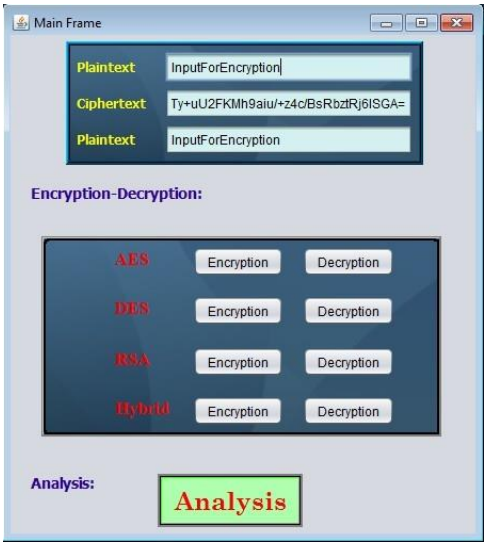

Fig 2: Main frame

Avalanche effect

In cryptography avalanche effect means amount of variation in cipher text by changing plain text with small extend.When an input is changed slightly then avalanche effect is evident. In height quality block cipher small change in either the key or the plaintext should drastic change in the cipher- text. We have calculated avalanche effect comparing two cipher-text generated from two plain text with slight difference using string comparison function. For our proposed

system we have calculated the avalanche effect separately for AES, DES, RSA and hybrid AES-DES-RSA and plotted it on histogram, what we found that hybrid algorithm has avalanche effect as good as AES. So considering future constrains of security we concluded that hybrid algorithm is better than the other cryptographic algorithm.

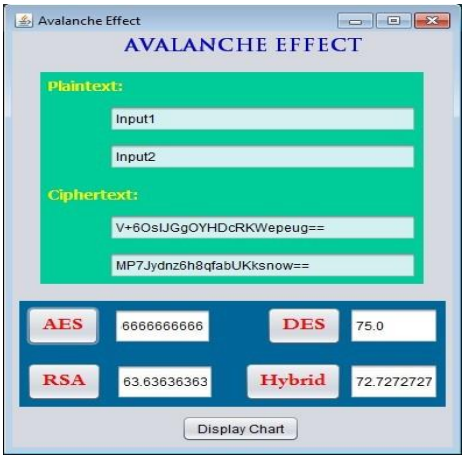

Fig 3: Avalanche Effect

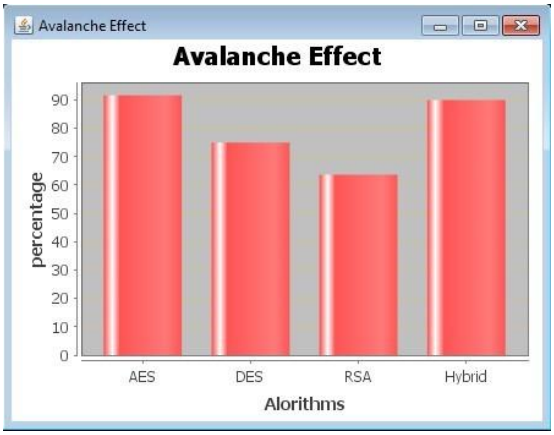

Fig 4: Plotted Histograms for avalanche effect

Throughput

In general terms, throughput is the rate of production or the rate at which something can be processed. In context of Encryption throughput is the rate at which data is getting encrypted. It is better to have high encryption throughput. As high Encryption rate(throughput) it is safe to transmit data through network. We have derived a approach to compute throughput i.e. (Total Number of Bits getting Encrypted) / (Total CPU Time).

In our proposed system we have plotted the histogram for the throughput parameter and we found that hybrid algorithm has better throughput as compared to the other cryptographic algorithm considering future security constrains it is better to adopt hybrid algorithm.

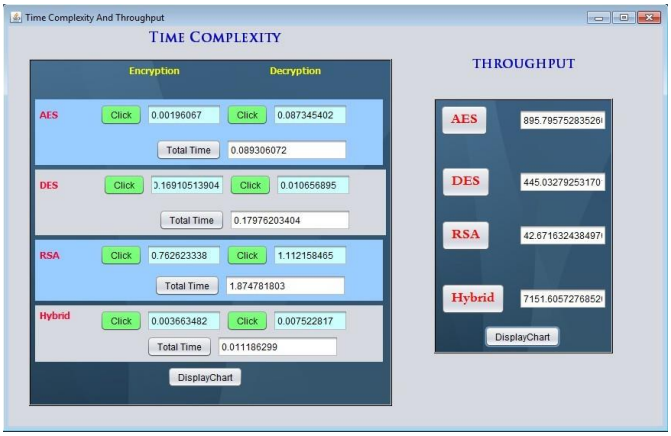

Fig 5: Time complexity and Throughput frame

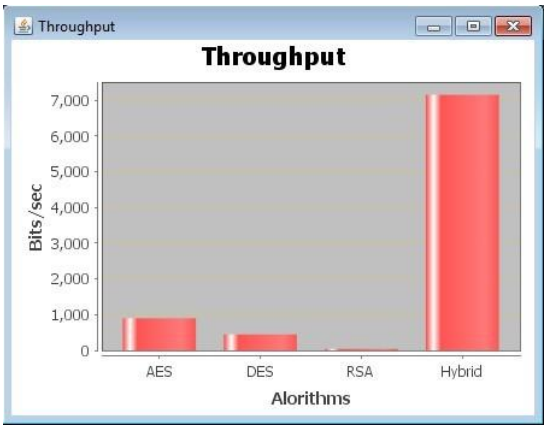

Fig 6: Plotted histogram for throughput

CPU Usage

CPU usage is amount of time required for completing different process in cpu for execution. Here we implement a hybrid algorithm for this algorithm we can calculate cpu usage in kilobytes and megabytes which can be shown in bellow graph

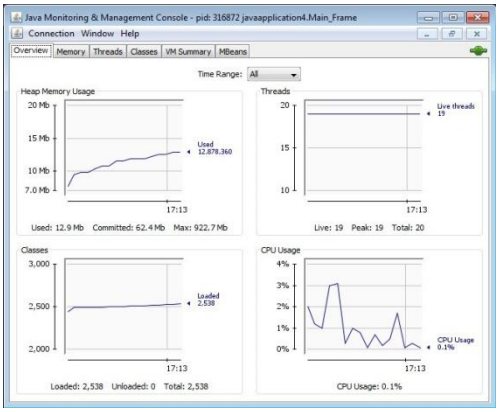

Fig 7: Memory Usage

Time Complexity

Encryption time is variable according to key size of algorithm. Here in the case of hybrid algorithm encryption time is minimized.

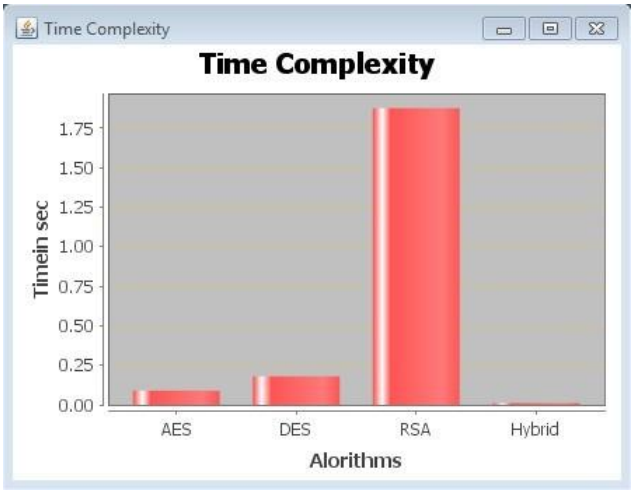

Fig 8: Plotted Histogram for Time complexity

VIII. CONCLUSIONS

We combined concept of AES-DES Algorithm and passing the encrypted data over network using RSA key exchange key mechanism. We have de-rived new Algorithm for transmitting data and achieve more security. Our Hybrid Algorithm is best option over three individual Algorithms as it over comes the drawbacks of each. Thus the hybrid approach which we developed is a better DES is merged with plain AES providing better diffusion. Thus the hybrid approach has better diffusion because DES is providing non-linearity to the simple AES. Brute force attack is nearly reduced by great extent as compare to rest three algorithms. Encryption time for hybrid is more than that of individuals as it uses the feistel structure incorporated with AES and then transmitted by RSA. Thus in all four parameters i.e. Avalanche effect, CPU Usage, Throughput and Encryption time, the proposed Hybrid Algorithm performs better.

REFERENCES

[1] Neal Krawetz, Introduction to Network Security, Charles River Media.
[2] https://autonome-antifa.org/IMG/pdf/Rijndael.pdf
[3] file:///C:/Users/admin/Downloads/differential%20cryptanalysis%20of%20des-like%20cryptosystems.pdf
[4] http://people.csail.mit.edu/rivest/Rsapaper.pdf
[5] Behrouz A. Forouzan, Data Communications And Networking, Mcgraw-Hill.