International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

Hybrid Model for Security Enhancement

Yash Shah[1], Rutuja Patil[2], Riddhi Rane[3] and Siddhesh Kharade[4]

[1]Assistant Professor, [2,3,4] Student
[1,2,3,4]Department of Information Technology, Vidyalankar Institute of Technology, Mumbai, Maharashtra, India

---

Abstract - With the exchange of data in electronic way, it has become a necessity to keep our data in a secured way. The hybrid cryptography algorithm aims to build an efficient and secure encryption algorithm based on merging the encryption algorithm to make hybrid encryption algorithm that can encrypt and decrypt data efficiently and in secure manner.

This paper presents Hybrid (AES & DES) encryption algorithm to safeguard data security. To make the algorithm more secured the key generation technique used is complex. This has helped in avoiding any chances of repeated or redundant key.

Key Words: AES, DES, Avalanche effect, Cryptography.

1.INTRODUCTION

Due to the rapid usages of data communication, security is becoming a more crucial issue. The fundamental requirements for security include authentication, confidentiality, integrity, and non-repudiation. To provide such security services, cryptography is the foundation and most system uses two major classes of cryptographic algorithms namely private-key and public-key algorithms. They usually operate at relatively high speed and are suitable for bulk encryption of messages. Public-key algorithms are based on the idea of separating the key used to encrypt a message from the one used to decrypt it. They are relatively slow and therefore unsuitable for encryption of large bulky messages.

Security becomes a very important issue in data transmission and there are so many methods to make files more secure. One of that method is cryptography the original file. Cryptography is derived from a Greek word which means, the art of protecting information by transforming it into an unreadable format. To prevent our data from unwanted users to get access to our data we need cryptography. Cryptography is associated with the process of converting original plain text into not human readable format. It is a process of transmitting data in a form that only those who can access the data can read and process it. Cryptography is a method to secure data by writing the hidden code to cover the original file.

The aim of the research project is to encrypt and decrypt data efficiently and effectively protect the transmitted data. This model uses the AES and DES security algorithm that encrypt and decrypt transmitted data. The proposed hybrid cryptography algorithm aims to build an efficient and secure encryption algorithm based on merging the encryption algorithm to make hybrid encryption algorithm that can encrypt and decrypt data efficiently and in secure manner.

2. METHODOLOGY

This project introduces hybrid approaches by combining two most important algorithms AES algorithm and DES algorithm. This hybrid encryption algorithm provides more security as compare to other security algorithm. The parameter on which this algorithm is analyzed was Avalanche effect, Bit Independence criteria and time consumed. In order to ensure more security the key which is given to this algorithm by the user in the beginning is given to a random function which generates more complex key which is then given to this hybrid algorithm. This provides more security.

The project studies the different set of algorithm and its implementations and examines it on some parameters which is time consumed, avalanche effect and bit independence criteria on the basis of above parameters a new hybrid algorithm is developed.

It provides more security as the key which the user enters is given to a random function which generates a more complex key which is then given to the hybrid algorithm.

2.1 Avalanche Analysis

The avalanche effect property is very important for encryption algorithm. This property can be seen when changing one bit in plaintext and then watching the change in the outcome of at least half of the bits in the cipher text. One purpose for the avalanche effect is that by changing only one bit there is large change then it is harder to perform an analysis of cipher text, when trying to come up with an attack.

$$\text{AvalancheEffect} = \frac{\text{Number of flipped bits in ciphered text}}{\text{Number of bits in ciphered text}}$$

2.2 Bit Independence Criteria

A second property which would seem desirable for any cryptographic transformation is that, for given set of avalanche vectors generated by the complementing of single plaintext bit, all the avalanche variable should be pair wise independent. In order to measure the degree of independence between a pair of avalanche variable, we calculate their correlation coefficient, if its zero it mean that the variable are independent, if its 1 that mean stronger positive correlation and -1 is stronger negative correlation.

3. PROPOSED SYSTEM

A method that follows two encryption and decryption algorithm that are AES and DES by using symmetric key.

3.1 Encryption

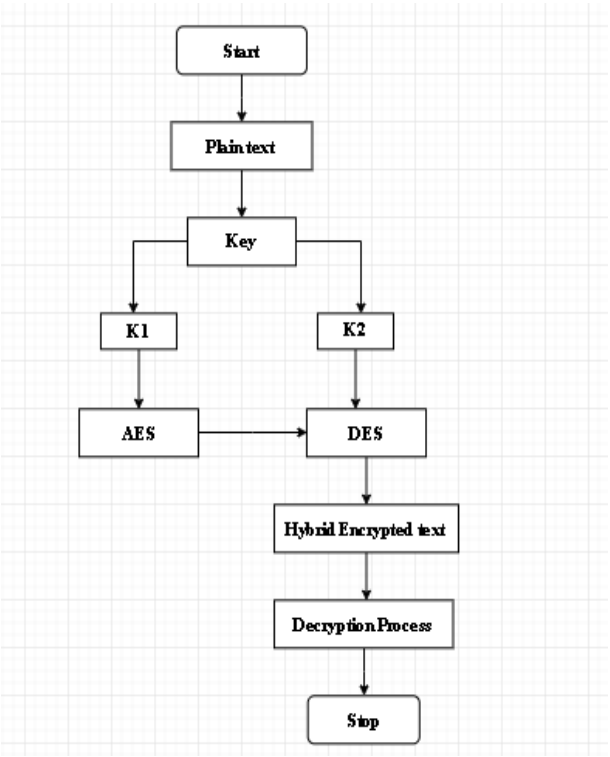

Fig-1: Flow chart of Encryption Process

Step1: The user will upload the file which is to be encrypted.

Step2: He will also enter the key 'K'.

Step3: The Key which is entered is divided into two parts 'K1' and 'K2' and given to the key generation process .

Step4: After the operations of key generation are performed K1 key is given to AES algorithm and K2 key is given to DES algorithm.

Step5: Then AES encryption is performed on the plain text and later DES algorithm is performed on it which results into hybrid encrypted text.

Step6: In this step, the result of the above step is given to the decryption process for further operations.

3.2 Decryption:

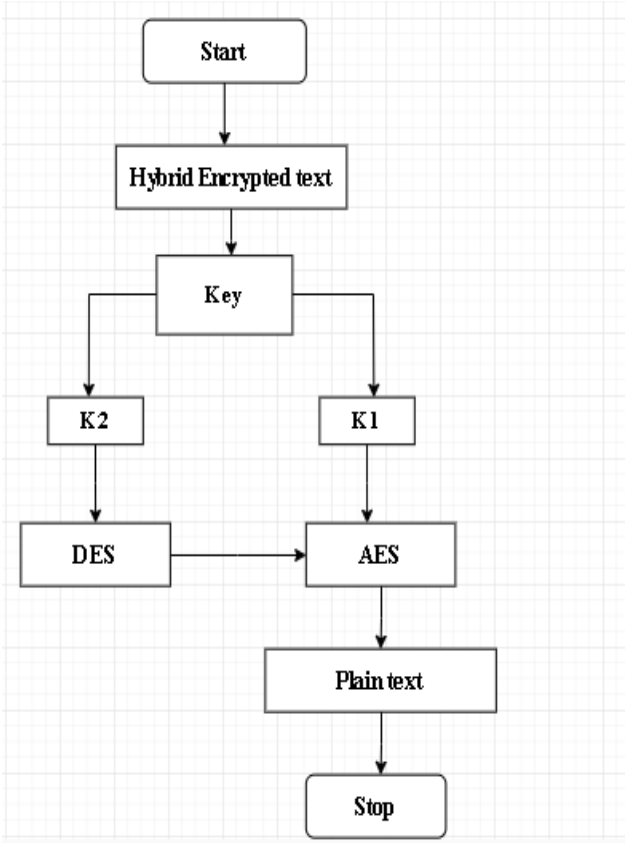

Fig-2: Flow chart of Decryption Process

Step1: The resultant hybrid text in the encryption process is given in this step of the decryption process.

Step2: The user is been asked to enter the same key which he entered at the beginning of the encryption process.

Step3: The entered key is divided into two parts 'K1' and 'K2' and key generation process is performed on it.

Step4: After key generation process K2 is given to DES algorithm and K1 is given to AES algorithm.

Step5: First DES is performed on the hybrid encrypted text and later AES is performed on it.

Step6: The above step result into plaintext which is similar to the plain text which user had uploaded

3.3 Key Generation

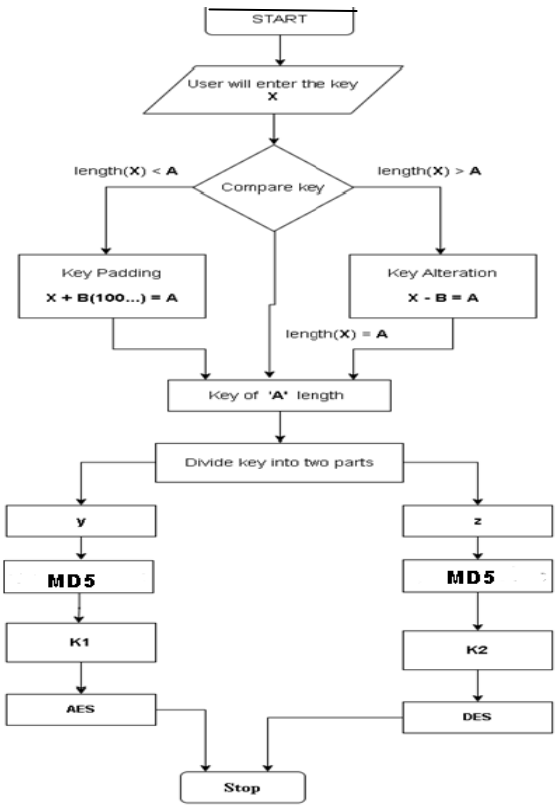

Fig-3: Flow chart of Key Generation process

Step1: The user will enter the key of any length and it will be denoted by X.

Step2: We will compare the length of the input that is length(X) with A. (A is the specific length decided)

- **Condition1**: If length(X) < A

Key padding will be performed until the length of X is equal to A size.

X + B (100..) = A

Where, 'B' are extra bits which are added.

- **Condition2**: If length(X) > A

Key alteration will be performed until the length of X is equal to A size.

X - B = A

Where, 'B' are bits which are eliminated.

Step3: After step2 is performed we will get a key of length A.

Step4: The key which is obtained in the above step is divided into two equal parts that is y and z.

Step5: y will be given to MD5 algorithm to perform hashing function.

Step6: z will be given to MD5 algorithm to perform hashing function

Step7: The result of above two steps is termed as K1 and K2 respectively.

Step8: K1 is further given to AES algorithm during encrypt ion and decryption process.

Step9: K2 is further given to AES algorithm during encryption and decryption process.

Step10: Key generation process ends here.

4. RESULT AND ANALYSIS

SR.NO	PLAINTEXT	BIT CHANGE	AVALANCHE EFFECT
1	1101000110010 11111001 (hey)	37	57.8%
	1101000110010 11111000 (hex)		
2	1100101110111 0110001111100 1011110011110 0001110100 (encrypt)	29	51.7%
	1100101110111 0110001111100 1011110011110 0001110110 (encrypy)		
	1100110110100 1110110011001		

3	01 (file)	32	50%
	1100110111100 1110110011001 01 (fyle)		
4	1100011110100 1111000011010 0011001011110 010 (cipher)	34	53.1%
	1100011110100 1111000011011 0011001011110 010 (cipler)		
5	1100110110100 1110111011000 01101100 (final)	38	59.3%
	1100110110100 1111111011000 011101100 (fi~al)		
AVERAGE			**54.38%**

Table-1: Results of avalanche effect of Hybrid algorithm

According to the analysis performed the avalanche effect calculated for Hybrid algorithm is 54.38%.

5.CONCLUSION

Using a combination of cryptography encryption algorithms such as AES and DES with SHA256 is one of secure and convenient technique for secure data via cloud storage services and achieve the confidentiality, integrity and non-repudiation. In the future, we will try to apply this method using GPU scheduling concepts to reduce the execution time for encryption and decryption phases. So this hybrid algorithm can be further used to transmit the encrypted data on the cloud. Moreover the proposed complex key generation in this project will further increase the security of the entire system.

REFERENCES

[1] Mohamad Noura, "DES: An efficient and secure DES Varient", 20188371019/
[2] Shady Mohameed Soliman,"Efficient implementation of the AES algorithm for security applications", 2017.
[3] Bawna Bhat,"DES and AES performance evaluation", 2015.
[4] Akash Kumar Mandal,"Analysis of Avalanche effect in plaintext using binary codes",2013.
[5] Seung-Jo Han, "The improved Data Encryption Standard algorithm(DES) ", 2012.
[6] B.Thiyagarajan, "Data Integrity and Security in Cloud Environment Using AES Algorithm",ICICES 2014.
[7] Takanori Machida, "Modifications to AES Algorithm for Complex Encryption", IEEE transactions 2015.
[8] C. Giraud, "An Implementation of DES and AES,Secure against Some Attacks", c Springer-Verlag Berlin Heidelberg.CHES, LNCS 2162, pp. 309–318, 2001.
[9] Shraddha Soni, "Analysis and Comparision between AES and DES Cryptographic Algorithm", December 2012.