Hybrid AES Algorithm with Enhanced Security for Heterogeneous Data

Priyanka Pandey, R. R. Sedamkar

Abstract*: This paper, presents the intricate Hybrid AES encryption method. Proposed algorithm's design and evaluation of security enhancement is done by implementing and comparing Dynamic S-box with Round structure & Variable Key Cipher technique for heterogeneous data. AES is one of ciphering algorithm which is utilized for encryption, decryption of data to provide confidentiality for end to culminate data transmission. Improvement is finished in AES by modifying the S-box. The static S-box is created dynamic utilizing key programing with the repetition of variable cipher key. The improvement analysis relies on cryptography Time, decoding Time and Throughput. Performance enhancement for security is evaluated for all the four algorithms- AES, AES with Round structure, AES with Variable Key cipher and our proposed Hybrid algorithm- AES with Round Structure and Variable key Cipher. Here focus is to make system attack resistant & secure data from assailers.

***Index Terms*: AES; S-box; Dynamic S-box, Round structure, Variable Key Cipher**

I. INTRODUCTION

In today's Modern Era, data is most precious factor of today's business. As the involution of the system & network are incrementing, susceptibilities are withal incrementing & task of securing the network is essential. The Advanced Encryption Standard or AES is a symmetric block cipher used to forfend relegated information and is implemented in software and hardware throughout the world to encrypt sensitive data. The focus of this research study will be done for making the system more attack resistant by the proposed Hybrid AES algorithm which can cope up to make AES cryptographically vigorous by utilizing dynamic Sbox with round structure and variable key Cipher. There are many recently researched types of Algorithm in AES like Advanced Encryption Standard (AES) Cipher suites for Convey Layer Security (TLS), Rijindael AES's [1], AES with Variable Key Cipher [3], and AES with Dynamic S-box [4]. We are fixating on cumulating two of them namely, AES with round structure & Variable key Cipher Model Development.

AES is one of the encryption techniques which are utilized most frequently because of its high efficiency and simplicity. It is the highly safe algorithm. Due to the potent increase in the cyber world and other modes of electronic communication, electronic security has turned progressively foremost. The science or art which circumvents the principles and methods of converting an intelligible message into unintelligible and then reconverting those messages back to their pristine form so as to store messages secure is called Cryptography. Cryptography is utilized to secure e-mail, messages, credit card info, and corporate information within the context of any application-to-application communication.

Advanced Encryption Standard not only assures security but additionally amends the performance in a diversity of settings such as smartcards, hardware implementations etc. AES is federal information processing standard and there are currently no kenned no brute-force direct attacks against AES. The 168-bit Digital Encryption Standard (3-DES) or the more incipient Advanced Encryption Standard (AES) are utilized in many system standards because it designates that, system should be attack resistant and data should be encrypted [9]. Many researchers have taken interest in the field of coalescing other encryption algorithms with AES. So, it can be considered as a motivational factor for further enhancement of AES. To enhance security of system's data, we have fixated on encryption of data, variable key cipher, round structure and dynamic s-box. Here, an incipient approach of nonlinear transformation algorithm for AES S-Box to enhance the involution of the S-Box structure, AES algorithm is made more vigorous by utilizing Dynamic S-box, with look up table S-box and Key expansion as modified when the initial key is transmuted, which when utilized with variable key cipher provides a better encryption algorithm The AES is utilized in Round structure for proposed system. The proposed algorithm engenders dynamic S-box to enhance AES algorithm. The cipher key is utilized to convert static S-box into dynamic. Analysis of algorithm is done on the substructure of sundry parameters. The parameters are encryption time, decryption time, and throughput.

II. BACKGROUND

Cryptography is that the art and science of keeping data secure. The required basic definitions and concepts [23] in Cryptography are reviewed here.

1. **Plaintext**: An original message is called Plaintext or clear text. It is denoted by M [a stream of bits, a text file, an image, etc.
2. **Encryption**: Process of disguising a message M in such a way as to hide its substance. The encryption function is given by, Ek (M) = C, E where k is key.
3. **Cipher text**: An encrypted message is Cipher text and denoted by C.
4. **Decryption**: Process of turning Cipher text back into Plaintext is called Decryption. The decryption function is given by, Dk (C) = M, D where k is key.

Revised Version Manuscript Received on 06 June 2018.

Priyanka Pandey, Thakur College of Engineering & Technology, Mumbai (Maharashtra), India.

Dr. R. R. Sedamkar, Thakur College of Engineering & Technology, Mumbai (Maharashtra), India.

III. ADVANCE ENCRYPTION STANDARD

The Advanced Encryption Standard, an algorithm also known as Rijndael after its inventors Vincent Rijmen and Joan Daemen. This algorithm works on 128-bit blocks and can use a key of 128, 192 or 256 bits in length. For encryption, each round consists of the following four steps:

1) Substitute Byte: Each byte in matrix is changed using 8-bit substitution box i.e. Sbox.
2) Shift Rows: A linear mapping that rotates on the left all the rows of matrix.1st row is keep as it is, 2nd row rotates by 1,3rd row rotates by 2 and4th row rotates by 3.
3) Mix Columns: Every column of input matrix is multiplied by the mix Column matrix that provides the corresponding column of output matrix.
4) AddRoundKey: Round key was merged with state. For each round key is acquired from main key through key scheduling; the round key is added by merging each byte of state with corresponding byte of round key using bitwise XOR.

IV. AES S BOX

The Rijndael S-box is a matrix i.e. square array of numbers used in the Advanced Encryption Standard (AES) cryptographic algorithm. It accommodates as a lookup table. Substitution is a nonlinear transformation which performs mystification of bits. S-box is shown as a 16x16 array, rows and columns indexed by hexadecimal bits. The S-box is the substitution box which accommodates as a lookup table. The S-box is engendered by determining the multiplicative inverse for a given number in GF (28). GF (28) = GF (2)[x]/(x8 + x4 + x3 + x + 1)

V. AES DYNAMIC S BOX WITH ROUND STRUCTURE

Dynamic S-box is applied in the round structure of AES where a 256 bit data as Input to the system. Here the Input Data is divided into two blocks of 128 bits each. One Block is given as Input to the AES section of the System. The other Block is given as Input to the AES section of the System in the next round as per the round structure. This is done for 10 rounds respectively. These outputs are then combined together to form 256 bit block of encrypted data as shown in figure below.

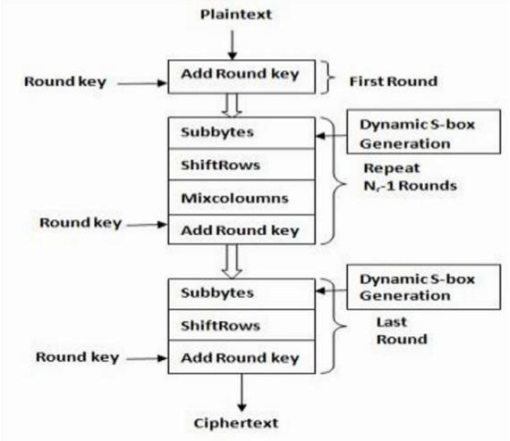

Fig 1. AES Dynamic S-box

VI. VARIABLE BLOCK KEY CIPHER

This technique is enhanced by utilizing variable key cipher wherever a stream of sub keys of AES is engendered from the pristine key with feedback from anterior cipher block and each sub block is encrypted with dissimilar sub keys. The utilization of variable key cipher makes the system nonlinear and engenders mystification within the utilization of keys.

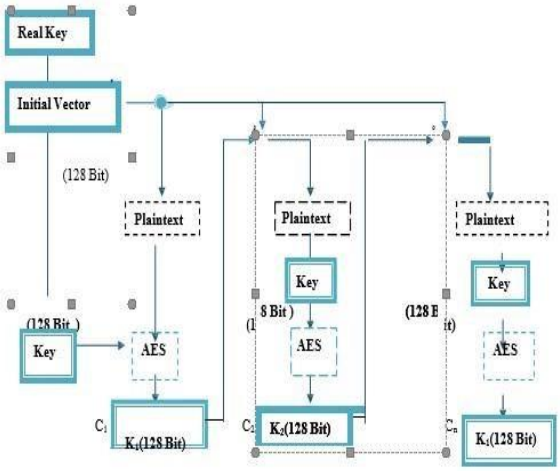

Fig 2. Key Generator

VII. PROPOSED HYBRID ALGORITHM

A high caliber proposed hybrid model as shown in Fig 3, wherein the Dynamic S-box is applied in the round structure of AES algorithm which is then cumulated with variable key block cipher to engender an incipient algorithm with high robustness.

VIII. LITERATURE SURVEY

In 2012, the paper [1], results show that the differential probability of the S-box is better than the subsisting S-box predicated on chaos, which has more vigorous opposition to differential attacks and nonlinear attacks, but not implemented on image and audio and Dynamic S-box. In 2013, paper [2] depicts the encryption and Decryption time is incremented, as well as the involution of network is incremented with the number of bits in one block. So the system can be utilized in the application where time is not the constraint. But it is not implemented with Model Key or Variable key cipher. In 2014, the paper [3], reviewed the first Incipient Cryptography algorithm & compares by parameter of throughput & Key Generation. But need to increment more number of Arithmetic & Logical operations with more throughput. In 2015, the paper [4] describes the major goal of this paper is the study of correlation in different cases of modified encryption techniques. But more depth study of different Enhancement of AES is required for Dynamic S-box Algorithm. In 2015, paper [5] shows that dynamic AES is found to be better than AES in terms of Arbitrariness & Correlation Co-efficient. But there is a desideratum to optimize the Dynamic s-box algorithm. In 2016, the paper [6], they had introduced dynamic S-box in lieu of static S-box for invigorating the algorithm to make it more secure.

There is a desideratum to optimize the Algorithm & search better way to Construct Dynamic S-Box. It solves the quandary of Anti fine-tuned point which was pristinely present in S-Box. In proposed system, we are coalescing the two technique namely, Dynamic S-box with round structure and variable key cipher and thus engendering the Hybrid Algorithm technique for heterogeneous data.

IX. PROPOSED SYSTEM

There are major drawbacks in pristine AES algorithms hence Hybrid AES algorithm is utilized in the proposed system because AES is the most secure algorithm. There are few attacks on the AES algorithm like linear, algebraic attacks hence to make the system more robust against attacks, AES is utilized in Round structure. The S-box of AES algorithm is ameliorated by making it dynamic. Here, the work is fixated on enhancement of subsisting AES's encryption algorithms by engendering a Hybrid one. The whole robust cryptographic system that has been developed in this project includes encryption of data, variable key cipher, and dynamic s-box and round structure. The performance evaluation will be done predicated on parameters like: Throughput, Encryption and Decryption Time with fine-tuned number of rounds (10) in the Round structure.

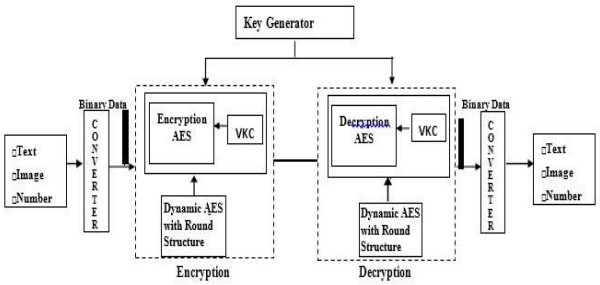

Fig 3. Proposed Hybrid-AES System

X. MODEL DEVELOPMENT

The flow of model development is as follows:

1) 256 bits key length is utilized for the Hybrid-AES algorithm.
2) The proposed system's encryption and decryption is equipollent to traditional AES algorithm.
3) The round function of encryption process is additionally homogeneous as the traditional AES algorithm.
4) There is additional phase of making S-box dynamic as shown in Fig. 1.
5) Before sub byte stage, the static S-box is converted into dynamic utilizing cipher key.
6) The round structure of AES is utilized as shown in Fig. 4
7) Dynamic S-box is applied in the round structure of AES as shown in Fig. 5 we take 256 bit data as Input to the system.
8) Here the Input Data is split into two blocks of 128 bits each.
9) One Block is given as Input to the AES section of the System.
10) The other Block is given as Input to the AES section of the System in the next round as per the round structure.
11) For Variable Key Cipher key generation as shown in Fig 6, it is initiated by inputting the Symmetric key; we denominate it as authentic key and then from the authentic key the first sub key K1 utilizing Key engenderer. Encrypt the first block of plaintext P1 by the AES utilizing K1 which engendered in the antecedent step followed by engendering from the authentic key the second sub key K2 utilizing Key Engenderer. Encrypt the second block of plaintext P2 by AES utilizing K2. Determinately, Engender the next sub key to encrypt the corresponding block of plaintext and reiterate this step until encrypt the last block in plaintext PN with sub key KN.
12) This is done for 10 rounds respectively.
13) These outputs are then cumulated together to compose 256 bit block of encrypted data.

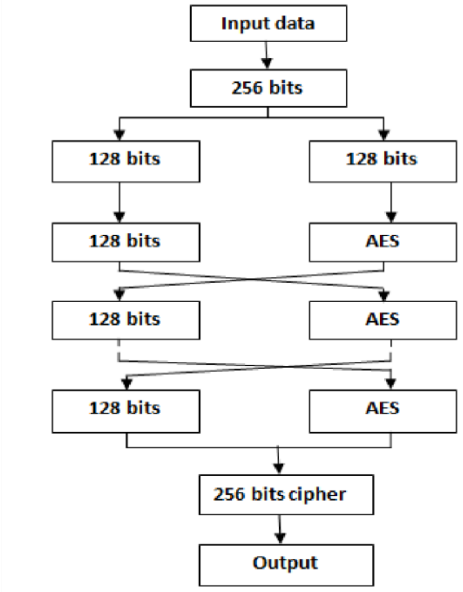

Fig 4. Round AES

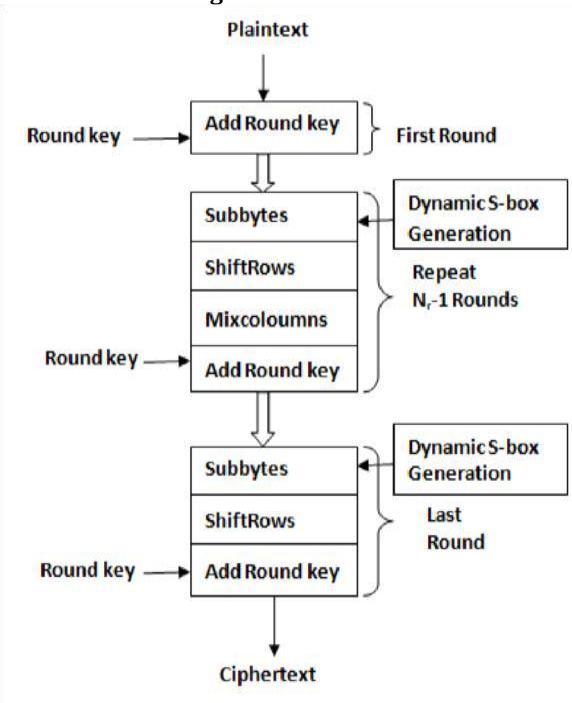

Fig 5. Round AES with Dynamic S-box

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

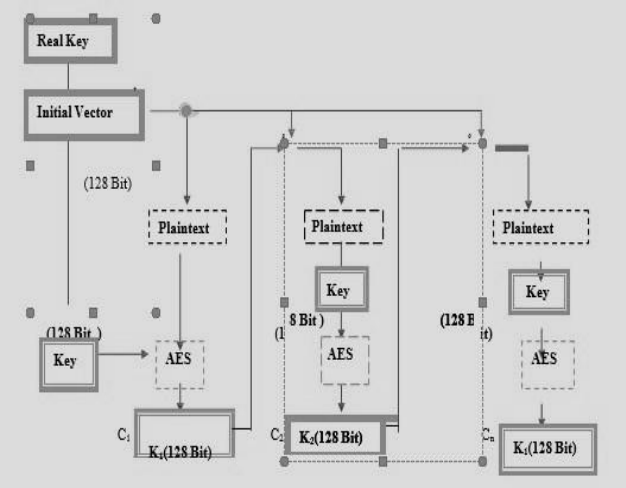

Fig 6. AES with Variable Key Cipher

XI. EXPERIMENTAL RESULT

The results carried out till the date is based on encryption time and throughput. Encryption time on input text file, number file and image file. Computer Configurations used are Microsoft Windows 7, Intel i5 CPU 3210M @ 2.50 GHz, 4 GB RAM and Matlab 2013a. For text file, "plaintext.txt" of 64 bytes, the number of bits is 512 and key is "enhanced aes key". The results are tabulated as shown below.

Table I. Based on Encryption Time on Text File

Algorithm	Bits in One Block	Plain text Size (bytes)	Plain text Size (kilo bytes)	No. of Blocks	Encryption Time (sec)	Decryption Time (sec)
AES	128	64	0.064	4	0.0175	0.009
AESRS	256	64	0.064	2	0.0031	0.0035
AES-VKC	128	64	0.064	4	2.4858	2.51
Hybrid AES	256	64	0.064	2	11.77	11.75

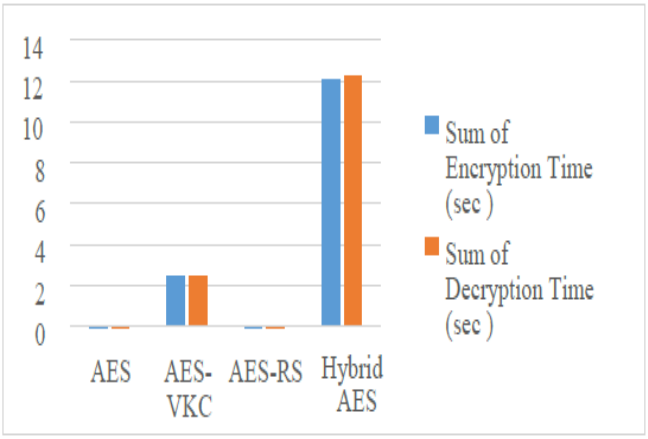

Fig 7. Graphical Representation of Results based on Encryption & Decryption Time on Text File.

For number file, "number.txt" of 64 bytes, the number of bits is 512 and key is "enhanced aes key

Table II. Based on Encryption Time on Number File

Algorithm	Bits in One Block	Plain text Size (bytes)	Plain text Size (kilo bytes)	No. of Blocks	Encryption Time (sec)	Decryption Time (sec)
AES	128	64	0.064	4	0.0021	0.0029
AESRS	256	64	0.064	2	0.004	0.0046
AES-VKC	128	64	0.064	4	2.4714	2.4908
Hybrid AES	256	64	0.064	2	12.021	12.21

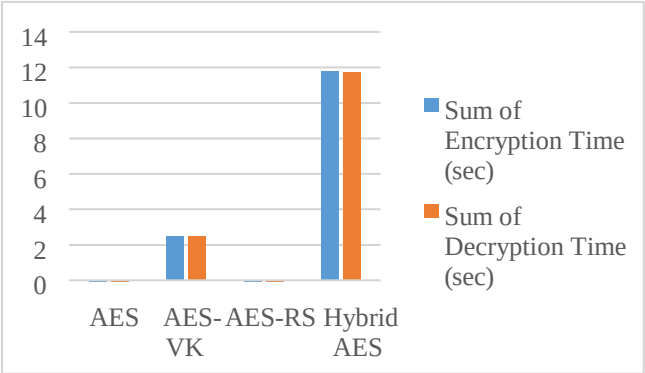

Fig 8. Graphical Representation of Results based on Encryption & Decryption Time on Number File.

For Image file, "Square Smile.jpg" of 3.01 KB, the number of bits is 24080 and key is "enhanced aes key".

Table III. Based on encryption time on image file

Algorithm	Bits in One Block	Image Size (Kilo bytes)	Image Size (bytes)	No. of Blocks	Encryption Time (sec)	Decryption Time (sec)
AES	128	3.01	3010	188	0.015	0.015
AESRS	256	3.01	3010	94	0.072	0.083
AES-VKC	128	3.01	3010	188	95.66	96.07
Hybrid AES	256	3.01	3010	94	503.5	505.96

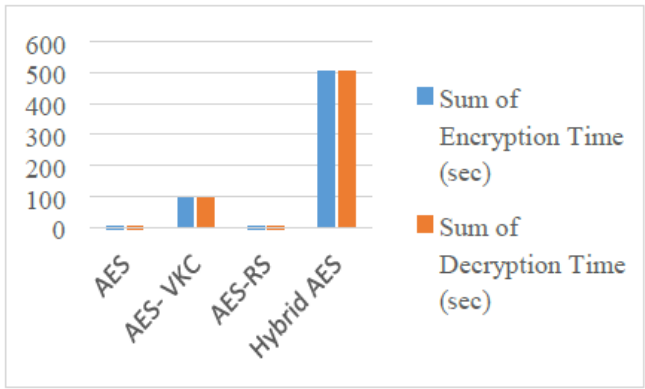

Fig 9. Graphical Representation of Results based on Encryption & Decryption Time on Image File.

Throughput on input text file, image file and number file. Computer Configurations used are Microsoft Windows 7,

Intel i5 CPU 3210M @ 2.50 GHz, 4 GB RAM and Matlab 2013a. For text file, "plaintext.txt" of 64 bytes, the number of bits is 512 and key is "enhanced aes key". The results are tabulated as shown below.

Table IV. Based on Throughput on Input Text File

Algorithm	Bits in One Block	Plaintext Size (bytes)	Plaintext Size (Kilo bytes)	No. of Blocks	Throughput (Encryption Time) Kbps	Throughput (Decryption Time) Kbps
AES	128	64	0.064	4	3.65	7.06
AES-RS	256	64	0.064	2	20.27	18.21
AES-VKC	128	64	0.064	4	0.02	0.02
Hybrid AES	256	64	0.064	2	0.005	0.005

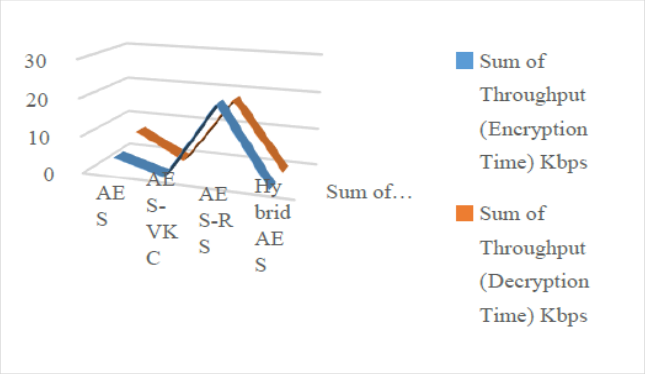

Fig 10. Graphical Representation of Results based on Encryption Time Throughput on Input Text File.

For number file, "number.txt" of 64 bytes, the number of bits is 512 and key is "enhanced aes key".

Table V. Based on Throughput on Number file

Algorithm	Bits in One Block	Plain text Size (byte s)	Plain text Size (kilo bytes)	No. of Blocks	Throughput (Encryption Time) Kbps	Throughput (Decryption Time) Kbps
AES	128	64	0.064	4	29.25	21.89
AESRS	256	64	0.064	2	16	13.91
AES-VKC	128	64	0.064	4	0.025	0.02
Hybrid AES	256	64	0.064	2	0.005	0.005

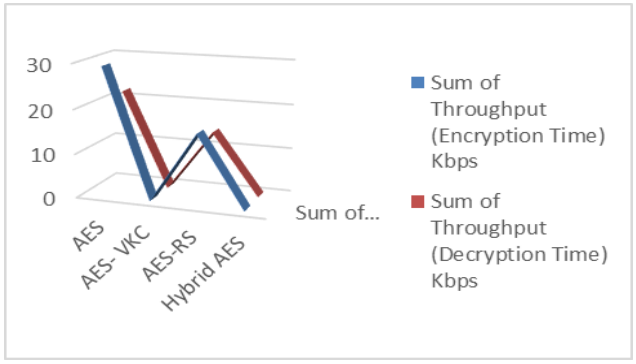

Fig 11. Graphical Representation of results based on Encryption Time Throughput on Input Number File.

For Image file, "Square Smile.jpg" of 3.01 KB, the number of bits is 24080 and key is "enhanced aes key".

Table VI. Based on Throughput on Image File

Algorithm	Bits in One Block	Image Size (Kilo bytes)	Image Size (bytes)	No. of Blocks	Throughput (Encryption Time) Kbps	Throughput (Decryption Time) Kbps
AES	128	3.0 1	3010	188	200.6	200.6
AESRS	256	3.0 1	3010	94	41.8	36.2
AES-VKC	128	3.0 1	3010	188	0.03	0.03
Hybrid AES	256	3.0 1	3010	94	0.005	0.004

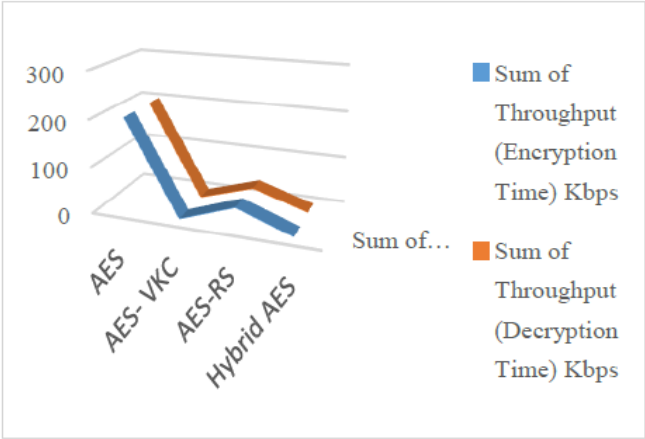

Fig 12. Graphical Representation of Results based on Encryption Time Throughput on Input Image File.

XII. CONCLUSION

In this paper, we introduced incipient potent algorithm for cryptography. This work is predicated on AES Hybrid encryption algorithm is enhanced by utilizing dynamic s-box with round structure and variable key cipher where a stream of sub keys of AES is engendered from the pristine key with feedback from precedent cipher block and each sub block is encrypted with totally different sub keys. The utilization of variable key cipher makes the system nonlinear and engenders perplexity in the utilization of keys. Then AES is utilized in Round structure for proposed system. The proposed algorithm engenders dynamic S-box to enhance AES algorithm. The cipher key is utilized to convert static S-box into dynamic. This is done to make AES cryptographically vigorous. This technique makes the algorithm more rebellious to brute force attack and additionally forfend from structural analysis, thus making the system more robust and assail resistant. Performance is evaluated predicated on heterogeneous data like Text file, Image file and Number file and result calculation is done on the configuration of Microsoft Windows 7, Intel i5 CPU 3210M @ 2.50 GHz, 4 GB RAM and Matlab 2013a. To enhance AES static S-box is converted into dynamic utilizing cipher key.

Hence we have concluded from the results that, when number of bits is incremented, the encryption time & decryption time is incremented and throughput is decremented as shown in the tables. Though encryption and decryption time is incremented, the intricacy of network is incremented with the number of bits in one block. So this system can be utilized in the application where time may or may not be the constraint.

We have engendered associate early hybrid formula by utilizing the two conjugation techniques of AES round structure and variable key cipher. The motivation behind incrementing involution is to create the system attack resistant and secure information from assailants. This is often the long term scope of the work.

ACKNOWLEDGMENT

I would like to thank Dr. R.R Sedamkar, Professor & Dean (Academics) for his valuable guidance and help. Sir's guidance and proficient motivation has helped me a lot during my research study.

REFERENCES

1. T. T. K. Hue T. M. Hoang and D. Tran, "Chaos-based S-box for lightweight block cipher//Communications and Electronics (ICCE)", IEEE Fifth International Conference IEEE, 2014.
2. Guo Guang-liang, Qian Quan, Zhang Rui, "Different Implementations of AES Cryptographic Algorithm," High Performance Computing and Communications (HPCC), (CSS), and (ICESS) 2015 IEEE 17th International Conference, 2015.
3. Scripcariu, L., "A study of methods used to improve encryption algorithms robustness," in Signals, Circuits and Systems (ISSCS) IEEE, 2015.
4. Nilesh D., Nagle M., "The new cryptography algorithm with high throughput," in Computer Communication and Informatics (ICCCI) IEEE, 2014
5. Chhotaray, S.K.; Chhotaray, A.; Rath, G.S., "A new method of generating public key matrix and using it for image encryption," in Signal Processing and Integrated Networks (SPIN), IEEE, 2015.
6. Schneider, Computer-and-network-security. WilsoN Publications, 2014. [28] Ed Skoudis, Top-computer and- network-security. Mc Graw Hill, 2015.
7. L. Stein, "Random patterns," in Computers and You, J. S. Brake, Ed. New York: Wiley, 1994, pp. 55-70.
8. Transmission Systems for Communications, 3rd ed., Western Electric Co., Winston-Salem, NC, 1985, pp. 44–60.
9. Karsanbhai, G.R, Shajan, M.G, "128 bit AES implementation for secured wireless communication," in Emerging Trends in Networks and Computer Communications (ETNCC),IEEE , 2011
10. S. Sahmod, W. Elmastry, S. Abudalta, "Enhance the Security of AES Against Modern Attacks by Using Variable Key Block Cipher" in International Arab Journal of e-technology, 2013
11. Daemen, "The Design of Rijndael-Advanced Encryption Standard", Nature 618.7532 (2015): 109110.
12. http://www.onlineprogrammingbooks.com/itsecurityaccessed 25-12-2016, 12:54 pm.
13. http://www.garykessler.net/library/crypto.htmlaccessed 25-12-2016, 12:58 am.