Advanced Encryption Standard (AES) Security Enhancement using Hybrid Approach

Flevina Jonese D’souza
M.E. Student, Computer Engineering
St. Francis Institute of Technology
Mumbai, India
flevi07@gmail.com

Dakshata Panchal
Assistant Professor, Computer Engineering
St. Francis Institute of Technology
Mumbai, India
dakshatapanchal@sfitengg.org

Abstract—**Security is major concern in data handling, communication, message transmission and electronic transaction on public network. Cryptography (secret writing) is the encryption process of transformation of messages to make information secure and resistant to attack. AES is symmetric encryption standard recommended by NIST. AES is proved to be highly secure, faster and strong encryption algorithm. AES is used commonly because of its great competence and easiness. But in recent years cyber-attacks are continuously developing, therefore security specialists must stay busy in the lab inventing new schemes to keep attackers at bay. Possible attacks on symmetric algorithm can be Brute-force Attack, Differential Attack, Algebraic Attack and Linear Attack. So to provide strong security in message transmission, AES algorithm with hybrid approach of Dynamic Key Generation and Dynamic S-box Generation is proposed. In hybrid approach first we will add more complexity in data to increase Confusion and Diffusion in Cipher text by using Dynamic Key Generation and then by using Dynamic S-Box Generation we will make it difficult for attacker to do any down study of static set of S-box.**

Keywords—AES; Decryption; Dynamic Key; Dynamic S-box; Encryption; S-box

I. INTRODUCTION

Cryptography (secret script) is the science and art of transformation of messages to make information secure and resistant to attack. Encryption is to guarantee safety of sensitive information. Encryption algorithm executes bytes substitutions and matrix transformations on the plaintext (original message before encryption) and converts it into cipher text (jumbled message). Information security can be handled using widely available encryption algorithms. The choice of key in cryptography is very vital since the security of encryption algorithm be determined by directly on it. Secrecy and Length of the key are important factors of the encryption key. A key can be numeric or alpha numeric text or may be a special symbol [1].

Advance Encryption Standard

AES is symmetric encryption standard recommended by NIST. AES supports Data Length of One hundred and twenty eight bits i.e. sixteen bytes and Key Length of one hundred and twenty eight bits, one hundred and ninety two bits, and two hundred and fifty six bits. AES goes through ten rounds for One hundred and twenty eight bit keys, twelve rounds for one hundred and ninety two bit keys and fourteen rounds for two hundred and fifty six bit keys. AES one hundred and twenty eight bit data length is separated into four operational blocks and treated as array of bytes, organized as matrix of 4*4 called State [1].

AES S-Box: The Rijndael Substitution-box is a matrix of Hex values used in the AES cryptographic algorithm. The s-box stands for substitution-box which is used as a lookup table. By determining the multiplicative inverse for a given number in GF (28) Rijndael's finite field the S-box is generated and is given by equation 1,

$$GF (28) = GF (2) [x]/(x8 + x4 + x3 + x + 1) \qquad (1)$$

Affine transformation is used to transform multiplicative inverse. This transformation is a vector in which sum of multiple rotations of the byte is taken, where sum is the XOR operation.

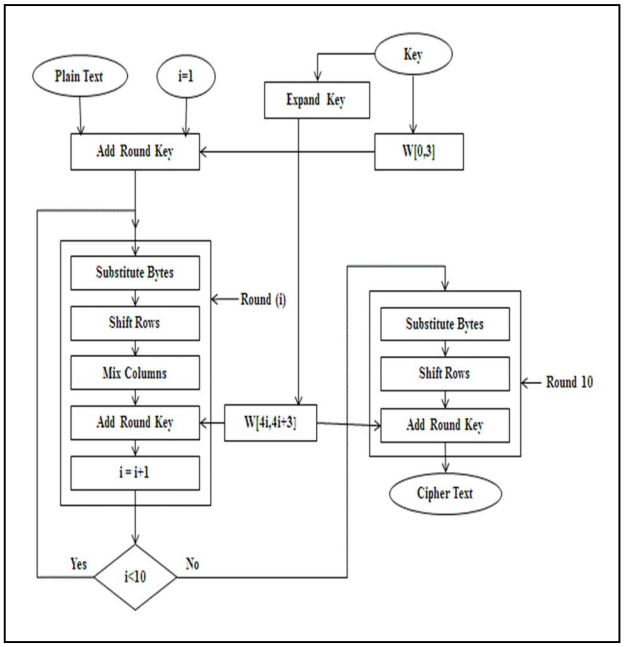


Fig. 1. Flowchart of AES [1].

Each round of AES has following transformations [2] and illustrated in Fig. 1:

ISBN: 978-1-5090-6471-7/17/$31.00 ©2017 IEEE

1. Substitute Byte Transformation

S-Box is used to transform each byte of data block into another block using substitution.

2. Shift Transformation of Rows

All row of the state matrix is cyclically left shifted based on their row position. (For 2nd row one byte, for 3rd row two byte and for 4th row three byte round left shift is executed)

3. Mix Transformation of Columns

It is matrix multiplication in which each column of the state matrix is multiplied with each column of fixed matrix.

4. Add Round Key Transformation

It is XOR operation between new state matrix and round key matrix.

II. Literature Survey

AES is most effective algorithm to provide security in message transmission. Singh et al. [1] studied three encryption algorithms like Rivest-Shamir-Adleman, Data Encryption Standard, Triple Data Encryption Standard and Advanced Encryption Standard to analyze effectiveness cryptography based on speed, time, and throughput and avalanche effect. Researchers proved that Advanced Encryption Standard is better algorithm than Data Encryption Standard, Triple Data Encryption Standard and Rivest-Shamir-Adleman for communication security.

Mahajan et al. [3] surveyed the performance of existing encryption techniques like Advanced Encryption Standard, Data Encryption Standard and Rivest-Shamir-Adleman algorithms. Based on the investigation researchers determined that Advanced Encryption Standard algorithm consumes least encryption and Rivest-Shamir-Adleman consumes longest encryption time. Also, Decryption of Advanced Encryption Standard algorithm is better than other algorithms. From the simulation result, it is estimated that Advanced Encryption Standard algorithm is greatly better than Data Encryption Standard and Rivest-Shamir-Adleman algorithm.

Padmavathi et al. [4] implemented three encryption algorithms like Data Encryption Standard, Advanced Encryption Standard and Rivest-Shamir-Adleman along with Least Significant Bit Substitution to analyze effectiveness cryptography based on encryption and decryption time and buffer usage. Researchers proved that Advanced Encryption Standard is better algorithm than Data Encryption Standard, Triple Data Encryption Standard and Rivest-Shamir-Adleman for communication security.

Musliyana et al. [5] have used Dynamic key generation in AES to solve attack vulnerability. Researchers proposed to use function of time. Key can be generated at random based on the value of the time when sender logs in to the system. On the decryption process takes a time value with a certain tolerance limits to find the same key pair of the time value generated in the encryption process. It provided stronger cipher key for AES encryption and decryption.

Juremi et al. [6] have proposed new design for Advanced Encryption Standard S-box which is used for bytes substitutions. Static substitute-box is transformed into dynamic substitute-box using cipher key. The inverse substitute-box will also be changed in the proposed system. This is done to make AES cryptographically strong. XOR operation of all bytes of cipher key is taken. The resultant Hex value will be used to rotate S-box. The proposed system introduced confusion in Advanced Encryption Standard to make it more complex. In this paper researchers have not performed cryptanalysis–attack (algebraic–attack) on this new technique.

Janadi et al. [7] proposed dynamic S-box method to increase the immunity of Advanced Encryption Standard algorithm against algebraic–attacks. Researchers introduced more complexity in the algorithm by using dynamic substitute-box.

Sahmoud et al. [8] have implemented algorithm to produce different sub keys from original key then every sub key is used in single round. It introduced more security against analysis attack such as brute force attack.

Major drawbacks of AES algorithm are:

- Cyber-attacks are continuously developing; therefore security specialists must stay busy in the lab inventing new schemes to keep attackers at bay [9].
- Symmetric algorithm can be broken by Brute-force Attack, Differential Attack, Algebraic Attack and Linear Attack [10][11][12].
- Breaking symmetric algorithm introduces the risk of intercepting or even impersonating & fraudulently verifying, private information.

In order to overcome the drawbacks of the original AES algorithm more enhancements to AES algorithm need to be developed which will consider the nodal demand.

III. Proposed Work

Due to the drawbacks in original AES, there arises the need for stronger encryption algorithm for security in message transmission. Therefore, we proposed the AES algorithm with hybrid approach (Dynamic Key Generation and Dynamic S-box Generation), which considers the nodal demands.

Flowchart of the proposed work advanced encryption standard security enhancement using hybrid approach is shown in Fig. 2.

The system will use 128 bits data and 128 bits key length. The sender will start the process by message transmission. The key will be dynamically generated based on function of time when sender logs in to system. In next step the S-box will be made dynamic by performing circular shift of it by value obtained after XOR on all bytes of round key. There will be added phase of creating S-box dynamic. Before substitute byte transformation stage, the static s-box will be transformed into dynamic using cipher key. For the decryption process, inverse S-box will also be changed from static to dynamic in similar way to dynamic S-box.

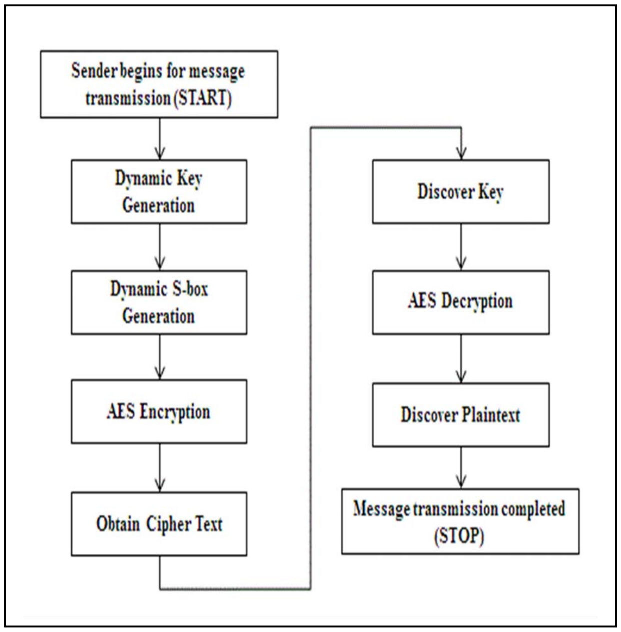


Fig. 2. Flowchart of the proposed work.

A. Dynamic Key Generation

Dynamic key is generated on AES algorithm using function of time. Key can be generated at random based on the value of the time when sender logs in to the system. On the decryption, synchronization activity takes time value with a certain tolerance limits to find the same key pair of the time value generated in the encryption process. It is illustrated in Fig. 3.

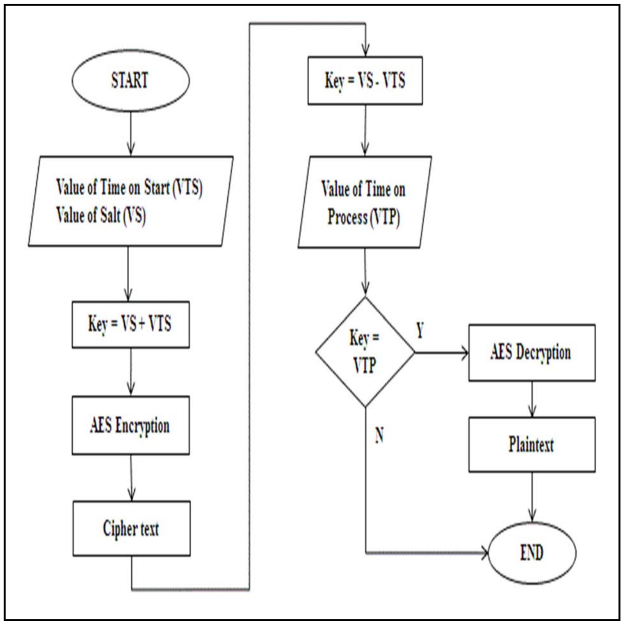


Fig. 3. Flowchart of dynamic key generation [5].

B. Dynamic S-Box Generation

Static substitute-box is transformed into dynamic S-box using cipher key. The inverse S-box will also be changed in the proposed system. This is done to make AES cryptographically strong. XOR process of all the bytes of cipher key is taken. The resultant Hex value will be used to rotate S-box. Fig. 4 shows the structure of Dynamic S-box generation.

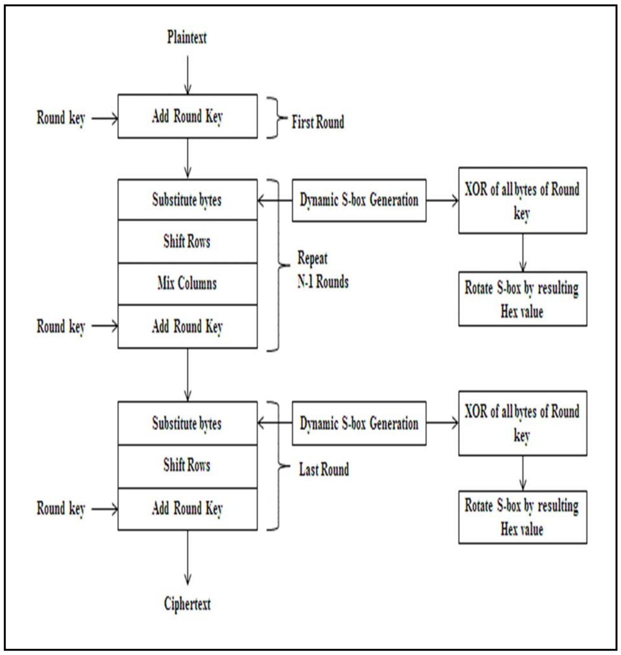


Fig. 4. Flowchart of dynamic S-box generation.

C. Example of Proposed Sysytem

Consider, plaintext to encrypt and decrypt using proposed system is **Two One Nine Two** (128 bits). And, cipher key to encrypt and decrypt using proposed system is **Thats my Kung Fu** (128 bits). The proposed system can be illustrated in below example explanation [13].

Key in English: Thats my Kung Fu
Hex: 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75
Key Matrix:

54	73	20	67
68	20	4B	20
61	6D	75	46
74	79	6E	75

Plaintext in English: Two One Nine Two
Hex: 54 77 6F 20 4F 6E 65 20 4E 69 6E 65 20 54 77 6F
State Matrix:

54	4F	4E	20
77	6E	69	54
6F	65	6E	77
20	20	65	6F

First Round Key:

w[0]= 54 68 61 74 **w[1]**= 73 20 6D 79 **w[2]**= 20 4B 75 6E **w[3]**= 67 20 46 75

Calculate g(w[3]):
Circular byte left shift of w[3] : 20 46 75 67
Byte substitution from s-box: B7 5A 9D 85
Adding round constant (01, 00, 00, 00) gives g(w[3]) : B6 5A 9D 85

w[4]= w[0] XOR g(w[3])= E2 32 FC F1
w[5]= w[4] XOR w[1]= 91 12 91 88
w[6]= w[5] XOR w[2]= B1 59 E4 E6
w[7]= w[6] XOR w[3]= D6 79 A2 93

1st Round key:
E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93

All Round keys:

Round 0	54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75
Round 1	E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93
Round 2	56 08 20 07 C7 1A B1 8F 76 43 55 69 A0 3A F7 FA
Round 3	D2 60 0D E7 15 7A BC 68 63 39 E9 01 C3 03 1E FB
Round 4	A1 12 02 C9 B4 68 BE A1 D7 51 57 A0 14 52 49 5B
Round 5	B1 29 3B 33 05 41 85 92 D2 10 D2 32 C6 42 9B 69
Round 6	BD 3D C2 87 B8 7C 47 15 6A 6C 95 27 AC 2E 0E 4E
Round 7	CC 96 ED 16 74 EA AA 03 1E 86 3F 24 B2 A8 31 6A
Round 8	8E 51 EF 21 FA BB 45 22 E4 3D 7A 06 56 95 4B 6C
Round 9	BF E2 BF 90 45 59 FA B2 A1 64 80 B4 F7 F1 CB D8
Round 10	28 FD DE F8 6D A4 24 4A CC C0 A4 FE 3B 31 6F 26

Encryption:

Round0: Add Round key
State Matrix XOR Round key0 Matrix

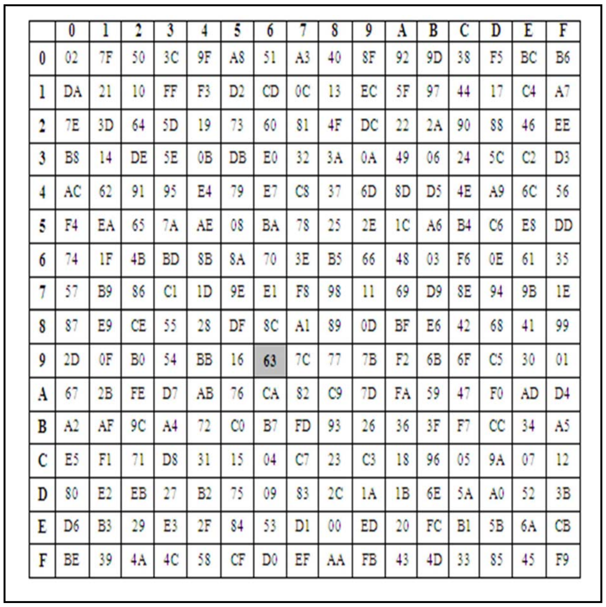
54	4F	4E	20		54	73	20	67
77	6E	69	54	⊕	68	20	4B	20
6F	65	6E	77		61	6D	75	46
20	20	65	6F		74	79	6E	75

New State Matrix

00	3C	6E	47
1F	4E	22	74
0E	08	1B	31
54	59	0B	1A

Round1:
Step1: Dynamic S-box Generation (consider key0)

54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75
XOR of all bytes is taken i.e. 6a (hex) or 106(Dec)
S-box is left shifted by 106 times.



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	02	7F	50	3C	9F	A8	51	A3	40	8F	92	9D	38	F5	BC	B6
1	DA	21	10	FF	F3	D2	CD	0C	13	EC	5F	97	44	17	C4	A7
2	7E	3D	64	5D	19	73	60	81	4F	DC	22	2A	90	88	46	EE
3	B8	14	DE	5E	0B	DB	E0	32	3A	0A	49	06	24	5C	C2	D3
4	AC	62	91	95	E4	79	E7	C8	37	6D	8D	D5	4E	A9	6C	56
5	F4	EA	65	7A	AE	08	BA	78	25	2E	1C	A6	B4	C6	E8	DD
6	74	1F	4B	BD	8B	8A	70	3E	B5	66	48	03	F6	0E	61	35
7	57	B9	86	C1	1D	9E	E1	F8	98	11	69	D9	8E	94	9B	1E
8	87	E9	CE	55	28	DF	8C	A1	89	0D	BF	E6	42	68	41	99
9	2D	0F	B0	54	BB	16	63	7C	77	7B	F2	6B	6F	C5	30	01
A	67	2B	FE	D7	AB	76	CA	82	C9	7D	FA	59	47	F0	AD	D4
B	A2	AF	9C	A4	72	C0	B7	FD	93	26	36	3F	F7	CC	34	A5
C	E5	F1	71	D8	31	15	04	C7	23	C3	18	96	05	9A	07	12
D	80	E2	EB	27	B2	75	09	83	2C	1A	1B	6E	5A	A0	52	3B
E	D6	B3	29	E3	2F	84	53	D1	00	ED	20	FC	B1	5B	6A	CB
F	BE	39	4A	4C	58	CF	D0	EF	AA	FB	43	4D	33	85	45	F9

Step2: Substitute Byte

02	24	61	C8
A7	6C	64	1D
BC	40	97	14
AE	2E	9D	5F

Step3: Shift Rows

02	24	61	C8
6C	64	1D	A7
97	14	BC	40
5F	AE	2E	9D

Step4: Mix Columns

78	5E	77	A4
27	7E	AA	C0
BA	81	6D	53
43	5B	5E	85

Step5: Add Round Key
Current State Matrix ⊕ Round key1 Matrix

78	5E	77	A4		E2	91	B1	D6
27	7E	AA	C0	⊕	32	12	59	79
BA	81	6D	53		FC	91	E4	A2
43	5B	5E	85		F1	88	E6	93

New State Matrix

9A	CF	C6	72
15	6C	F3	B9
46	10	89	F1
B2	D3	B8	16

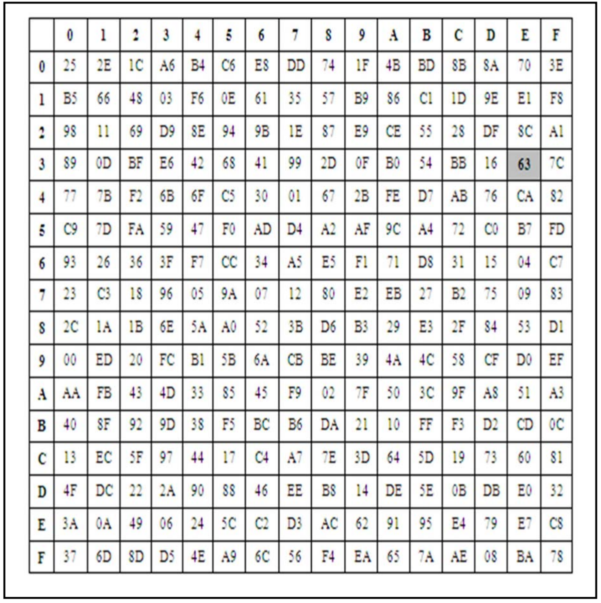
Similarly, round 2 to round 9 will be performed.

State Matrix after Round 9:

5B	50	72	82
30	13	E8	D1
22	4E	0A	7C
FA	CA	26	28

Round10:
Step1: Dynamic S-box Generation (Consider key9)

BF E2 BF 90 45 59 FA B2 A1 64 80 B4 F7 F1 CB D8
XOR of all bytes is taken i.e. C2 (hex) or 194(Dec)
S-box is left shifted by 194 times.



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A	70	3E
1	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E	E1	F8
2	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF	8C	A1
3	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16	63	7C
4	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76	CA	82
5	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0	B7	FD
6	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15	04	C7
7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75	09	83
8	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84	53	D1
9	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF	D0	EF
A	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8	51	A3
B	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2	CD	0C
C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73	60	81
D	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB	E0	32
E	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79	E7	C8
F	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08	BA	78

Step2: Substitute Byte

A4	C9	18	1B
89	03	AC	DC
69	CA	4B	B2
65	64	9B	87

Step3: Shift Rows

A4	C9	18	1B
03	AC	DC	89
4B	B2	69	CA
87	65	64	9B

Step4: Add Round Key
Current State Matrix ⊕ Round key10 Matrix

8C	A4	D4	20
FE	08	1C	B8
95	96	CD	A5
7F	2F	9A	BD

Cipher Text: 8C FE 95 7F A4 08 96 2F D4 1C CD 9A 20 B8 A5 BD

Decryption:

Round0: Add Round key
State Matrix ⊕ Round key10 Matrix

8C	A4	D4	20		28	6D	CC	3B
FE	08	1C	B8	⊕	FD	A4	C0	31
95	96	CD	A5		DE	24	A4	6F
7F	2F	9A	BD		F8	4A	FE	26

New State Matrix

A4	C9	18	1B
03	AC	DC	89
4B	B2	69	CA
87	65	64	9B

Round1:
Step1: Inverse Shift Rows

A4	C9	18	1B
89	03	AC	DC
69	CA	4B	B2
65	64	9B	87

Step2: Inverse Substitute Byte

5B	50	72	82
30	13	E8	D1
22	4E	0A	7C
FA	CA	26	28

Step3: Add Round Key
Current State Matrix ⊕ Round key9 Matrix

5B	50	72	82		BF	45	A1	F7
30	13	E8	D1	⊕	E2	59	64	F1
22	4E	0A	7C		BF	FA	80	CB
FA	CA	26	28		90	B2	B4	D8

New State Matrix

E4	15	D3	75
D2	4A	8C	20
9D	B4	8A	B7
6A	78	92	F0

Step4: Inverse Mix Columns

E4	7E	5B	78
09	02	B1	FA
04	E2	8C	9E
28	0D	21	0E

Similarly, round 2 to round 9 will be performed.

State Matrix after Round 9:

02	24	61	C8
6C	64	1D	A7
97	14	BC	40
5F	AE	2E	9D

Round10:

Step1: Inverse Shift Rows

02	24	61	C8
A7	6C	64	1D
BC	40	97	14
AE	2E	9D	5F

Step2: Inverse Substitute Byte

00	3C	6E	47
1F	4E	22	74
0E	08	1B	31
54	59	0B	1A

Step4: Add Round Key

Current State Matrix ⊕ Round key0 Matrix

54	4F	4E	20
77	6E	69	54
6F	65	6E	77
20	20	65	6F

Plain Text: 54 77 6F 20 4F 6E 65 20 4E 69 6E 65 20 54 77 6F

Plain Text (Dec): Two One Nine Two

Above example shows that plaintext can be encrypted and decrypted using proposed system of AES with hybrid approach which will have enhance security of AES.

IV. CONCLUSION

The proposed AES algorithm with hybrid approach will be an effective technique for providing strong security in message transmission by adding more complexity in AES to increase Confusion and Diffusion in Cipher text. It will protect message from Brute-force Attack, Differential Attack, Algebraic Attack and Linear Attack. Proposed system will be an effective technique for the applications which are based on internet such as e-commerce online shopping, Stock Trading, Net Banking and Electronic bill payment and so on.

REFERENCES

[1] G. Singh and Supriya, "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security," International Journal of Computer Applications, vol.67, pp. 33-38, April 2013.

[2] P. S. Mukesh, M. S. Pandya and S. Pathak, "Enhancing AES algorithm with arithmetic coding," 2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), pp. 83-86, IEEE, 2013.

[3] P. Mahajan and A. Sachdeva, "A study of Encryption algorithms AES, DES and RSA for security," Global Journal of Computer Science and Technology, vol.13, pp. 14-22, 2013.

[4] B. Padmavathi and S. R. Kumari, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution," International Journal of Science and Research (IJSR), vol.2, pp. 170-174, April 2013.

[5] Z. Musliyana, T. Y. Arif and R. Munadi, "Security Enhancement of Advanced Encryption Standard (AES) using Time-Based Dynamic Key Generation," ARPN Journal of Engineering and Applied Sciences, vol.10, pp. 8347-8350 , October 2015.

[6] J. Juremi, R. Mahmod and S. Sulaiman, "A proposal for improving AES S-box with rotation and key-dependent," International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), pp. 38-42, IEEE, 2012.

[7] A. Janadi and D. A. Tarah, "AES immunity Enhancement against algebraic attacks by using dynamic S-Boxes," 3rd International Conference on Information and Communication Technologies: From Theory to Applications (ICTTA), pp. 1-6, IEEE, 2008.

[8] S. Sahmoud, W. Elmasry and S. Abudalfa, "Enhancement the Security of AES Against Modern Attacks by Using Variable Key Block Cipher," International Arab Journal of e-Technology, vol.3, pp. 17-26, January 2013.

[9] "Encryption and Decryption," [Online] Available: https://developer.mozilla.org/en-US/docs/Archive/Security/Encryption_and_Decryption [Accessed on December 28, 2016].

[10] V. Kaul, B. Nemade and V. Bharadi, "Next Generation Encryption Using Security Enhancement Algorithms for End to End Data Transmission in 3G/4G Networks," Procedia Computer Science, vol.79, p. 1051-1059, 2016.

[11] H. Alanazi, B. B. Zaidan, A.A. Zaidan, H.A. Jalab, M. Shabbir and Y. AI-Nabhani, "New comparative study between DES, 3DES and AES within nine factors," Journal of Computing, vol. 2, pp. 152-157, March 2010.

[12] A. Alabaichi and A. I. Salih, "Enhance security of advance encryption standard algorithm based on key-dependent S-box," 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC), pp. 44-53, IEEE, 2015.

[13] K. Lala, A. Kumar and A. Kumar, "Enhanced throughput AES encryption," IJECSE, vol. 1, p. 2132-2137, 2012.