SECURITY ANALYSIS OF AES AND ENHANCING ITS SECURITY BY MODIFYING S-BOX WITH AN ADDITIONAL BYTE

Abdullah Al- Mamun[1], Shawon S. M. Rahman, Ph.D.[2], Tanvir Ahmed Shaon[1] and Md Alam Hossain[1]

[1]Department of Computer Science and Engineering
Jessore University of Science and Technology,Jessore-7408,Bangladesh
[2]Associate Professor, Department of Computer Science
Majmaah University, Majmaah, Kingdom of Saudi Arabia

ABSTRACT

Secured and opportune transmission of data alwaysis a significant feature for any organization. Robust encryption techniques and algorithms always facilitate in augmenting secrecy, authentication and reliability of data. At present, Advanced Encryption Standard (AES) patronized by NIST is the most secure algorithm for escalating the confidentiality of data. This paper mainly focuses on an inclusive analysis related to the security of existing AES algorithm and aim to enhance the level security of this algorithm. Through some modification of existing AES algorithm by XORing an additional byte with s-box value, we have successfully increased the Time Security and Strict Avalanche Criterion. We have used random additional key for increasing security. Since this key is random, result of security measurement sometimes fluctuates.

KEYWORDS

Cryptography;Advanced Encryption Standard;secure algorithm;s-box; Ciphertext; Avalanche Effect; SAC;

1. INTRODUCTION AND HISTORY

Security is an issue to defend anything from danger or threat. From the very beginning of humankind, Security was major concern to protect valuable things. Nowadays information has become more and more important.Before 19th century information was stored as hard copy and people used physical media to store &classical cryptography to protect that. But in 20th century digital way was invented to store and share information using computer and Internet. Internet is a common place for storing & sharing data. Everyone has free accessibility to it. So there is a question to protect information from unauthorized access. And so, modern cryptography has initialized.

Cryptography is a way of storing and transmitting data in a scramble form that can only be understood and processed by intended persons [1][20]. The many schemes used for encryption constitute the area of study known cryptography. Such a scheme is known as cryptographic system or a cipher. Encryption is a process of secure one's data from unauthorized access. Our data in readable form is called plaintext; data in encoded or unreadable form is called cipher text.

DOI: 10.5121/ijcnc.2017.9206

The process of converting or translating plaintext to cipher text is called encryption and its reverse is called decryption. Figure 1 shows encryption and decryption process.

In modern cryptography, complex algorithms or functions are used for encryption and decryption. All these algorithms use keys of different size for encryption and decryption. The strength of cryptography depends on the algorithm and key used. The key can be private or public. In public key Cryptography, pair of key is used[20][21][22]. One key is private and other is public. Both sender and receiver generate their own pair of key. Receiver distributes the public key to the intended senders and keep private key secret. Sender encrypts data with receiver's public key and sends the ciphertext to the receiver. The receiver decrypts that ciphertext with own private key to generate plaintext. In private key cryptography same key is used for both encryption and decryption. The key is always kept secret. Sender encrypts the plaintext with the private key and sends to the receiver. The receiver decrypts the ciphertext with same key.

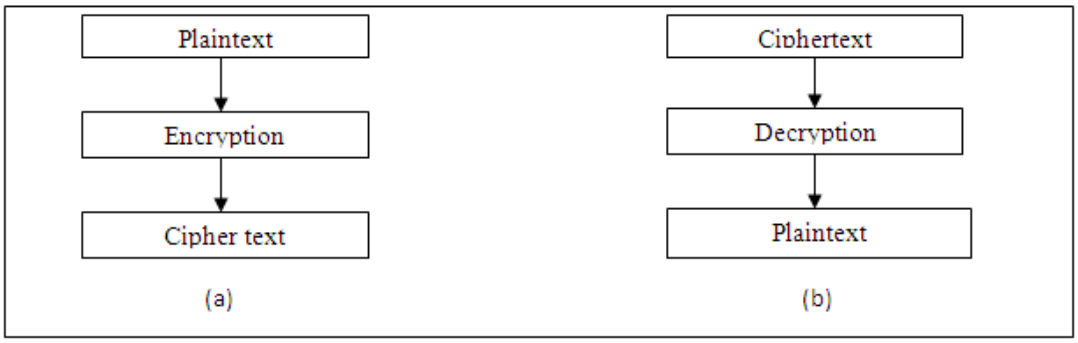

Figure 1 (a) Encryption Process (b) Decryption Process

2. BACKGROUND STUDY

2.1.AES Description

Advanced Encryption Standard (AES) is a symmetric cipher and it always uses the same key for encryption and decryption. This key is called cipher key. AES is also a block cipher and splits it input stream into block of fixed size. It allows a verity of block and key size. The size can be 128, 160, 192, 224 and 256 bits (multiple of 32 bits and from minimum 128 to maximum 256 [2]). But the standard is that, the input block size will always be fixed at 128 and the key size will be any of 128, 192 and 256. AES follows the substitution permutation network structure and so it has several working rounds depending on the key size. AES works in 10 rounds for 128 bits key, 12 rounds for 192 bits key and 14 rounds for 256 bits key. Nowadays, most commonly used key size is 128.

In inner work of AES, cipher key is expanded into 11, 13 or 15 keys respectively for 10, 12 or 14 rounds. Then the input block is copied into an array named state array. State array is 4x4 matrixes. Afterword the state array is XOR'ed with first round key and this step is known as AddRoundKey. Finally, AES perform 10, 12 or 14 rounds of computation on state array according to key size. Each round contains four different steps and last round contains three steps. AES steps are [3]:

1. Key expansions:**Rijndaelkey schedule**expands all round keysfrom cipher key.
2. Initial round: **AddRoundKey** – The state array is XOR'ed with the first round key.
3. Rounds: Each roundexcept last round performs these four steps.
   - **SubBytes** on state array using s-box.
   - A permutation **ShiftRows** on state array.
   - **MixColumns** on state array.
   - **AddRoundKey** with state array.
4. Final round: This round does not contain MixColumns and it performs following three steps.
   - **SubBytes** on state array using s-box.
   - A permutation **ShiftRows** on state array.
   - **AddRoundKey**with state array.

2.2.Key Expansion

In cryptography , each round consist of same set of operations but some parameter like cipher key or round key are different from each other. A Key Schedule is an algorithm that gives those round keys for each round [4]. Suppose, each word length w_i= 32 bits = 4 bytes. So a key consists of 4 words (4*32=128) and the initial round key is $w_0 + w_1 + w_2 + w_3$.

Others words will be calculated as follows:

$w_i = w_{i-1}$ Xor w_{i-4} for all values of i that are not multiple of 4.

For the words with indices that are a multiple of 4 (w_{4k}):

- RotWord: Bytes of w_{4k-1} are rotated left shift (nonlinearity).
- SubWord (r_{sw}): SubBytes function is applied to all four bytes (Diffusion).
- The result (r_{sw}) is XOR'ed with w_{4k-4} and round constant rcon.

That is: w_{4k}= r_{sw} Xor w_{4k-4} Xor r_{con}.

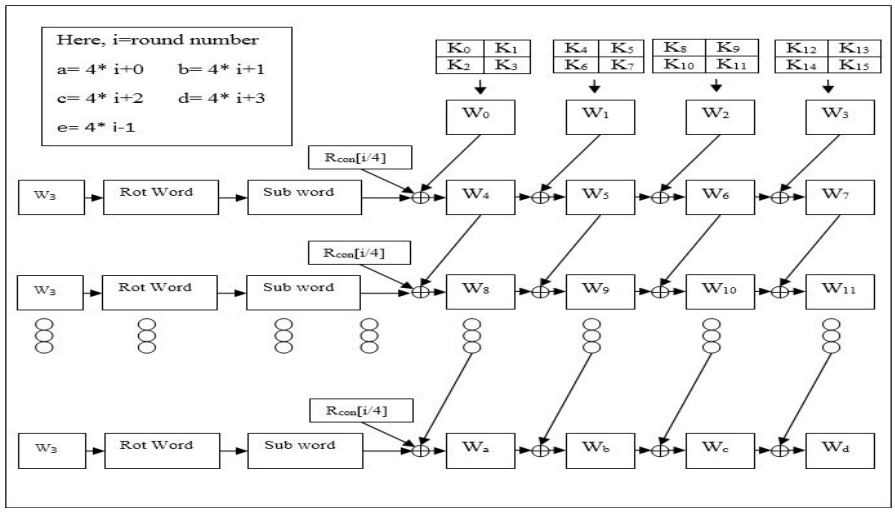

Figure 1. Diagram of Key Expansion

2.3.AddRoundKey

AddRoundKey is the initial step of encryption and decryption process. It is also a step in every rounds of AES algorithm. In AddRoundKey step, the plaintext array that means state array is being XOR'ed with round key. In this step 16 byte state array XOR'ed with 16 byte (4 words) round key and generate 16 byte (128 bit) output.

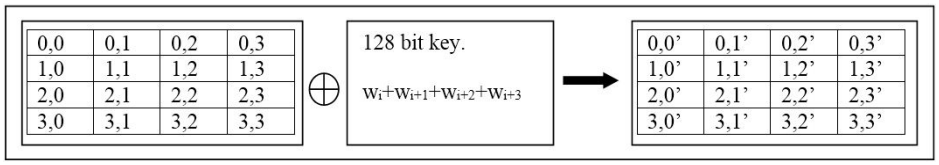

Figure 2. State array XOR'ed with Round Key

2.4.SubBytes

SubBytes mean substitution of byte of the state array by searching in lookup table which is called substitution box or S-box. S-box is a 16*16 lookup table and it contains 256 different values. The S-box table contains all possible values for 8 bit sequence that means in decimal 0 to 255.

Each byte of the state array is the input of this SubBytes step and the input byte is alternated by a corresponding value. Figure 4 shows S-box. Each byte is mapped into a new byte in the following way: the left most 4 bits denotes the row and right most 4 bits denotes the column of s-box. Suppose the input byte in s-box is b7 (in binary 10110111). The left most 4 bits means 1011 (b) denotes the row number and 0111 (7) denotes the column number of S-box. So the output value for input b7 is a9 (in binary 10101001)[5].

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 3. 16*16 Look up Table

2.5.ShiftRows

ShiftRows step perform shifting of bytes among the columns of a state array. The state array contains 4 rows and 4 columns. This step perform left shift of certain offset in different rows cyclically. For 128 bit and 192 bit data block ShiftRows rules are given bellow:

- First rows will be unchanged.
- Second row will be shift 1 byte to left.

- Third row will be shift 2 bytes to left.
- Fourth row will be 3 bytes to left.

In general, row 'a' is left shifted cyclically for (a-1) bytes.

For 256 bit block data ShiftRows rules step are:

- First rows will be unchanged.
- Second row will be shifted 1 byte to left.
- Third row will be shifted 3 bytes to left.
- Fourth row will be 4 bytes to left.

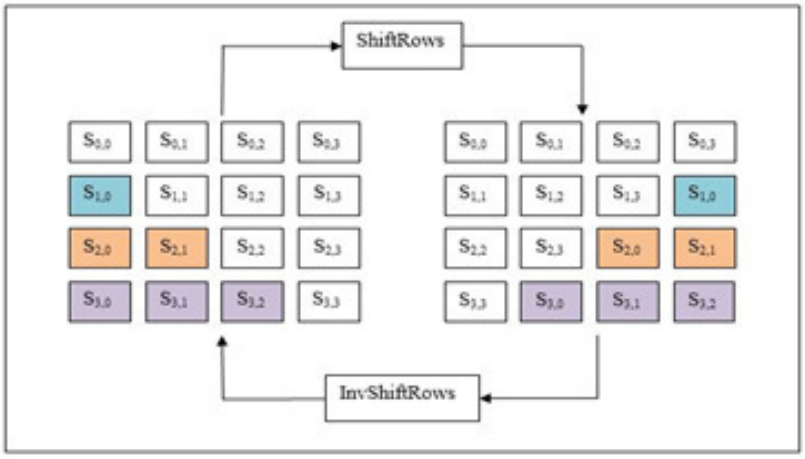

Figure 4. ShiftRows

The importance of this step is to avoid the columns being linearly independent.In decryption, the Inverse ShiftRows step perform opposite route shifting of each of the last three rows.

2.6.Mix Columns

MixColumns step offer diffusion in AES encryption. Each column of state array enters in MixColumns step and produces four output columns. This step takes a column of state array and performs matrices multiplication with a fixed matrix and produces an output column.

3.SECURITY MEASUREMENT CRITERIA

Security is the key term of Advanced Encryption Standard. Security of AES means how resistant this system is against active or passive attack. We measure the security based on three criteria [6].

- Time Security
- Avalanche Effect
- Strict Avalanche Condition

3.1.Time Security

It depict the potency of cryptographic method against brute force attack with different key size and time it takes to effectively mount a brute force attack.Brute force attack means thoroughly checking all probable key combinations until the accurate key is originate. For a 3 bit key, Brute force attack will take maximum 8 rounds to check every possible key arrangement. Maximum key combination for different key size is given in table 1.

From table 1, for 128 bit key brute force attack must check maximum 3.403 x 10^{38}key combinations. Now the brute force attacking time based on processing speed of latest super computer can be measured.

Table 1. Maximum Key Combination

Key size	Possible Combination	Key size	Possible Combination
1 bit	2	32 bit	4294967296
2 bit	4	64 bit	1.8447 x 10^{19}
4 bit	16	128 bit(AES)	3.403 x 10^{38}
8 bit	256	192 bit(AES)	6.278 x 10^{57}
16 bit	65536	256 bit(AES)	1.158 x 10^{77}

Faster Super Computer: 33.86 PFLOP/s = 33.86 x 10 ^{15} FLOP/s.

33.86 Quadrillion keys per second**.** [1 Quadrillion=1,000,000,000,000,000;one thousand million million; 10^{15}; prefix peta-]

1 year=365*24*60*60=31536000s.

So, 31536000*3.386 x 10^{16}= 1.067 x 10^{24}keys per year.

So, Brute force attack time to break 256 bit key is = $\frac{1.158e77}{1.067e24}$years

= 1.0844 x 10^{53}years

So 1.0844 x 10^{53}years need to break the 256-bit AES key using brute force attack

Table 2. Estimation of Years to Break AES

No	Key size	Years Need
01	128 bit	3.19 x 10^{14} years
02	192 bit	5.88 x 10^{33} years
03	256 bit	1.0844 x 10^{53} years

As shown in table 2, even with a supercomputer, it would take 1 billion billion years to crack the 128-bit AES key using brute force attack.

3.1.Avalanche Effect

Avalanche effect is a property that is very crucial for block cipher and cryptographic hashfunction. A cryptosystem has avalanche property if for flipping or change just a single bit in plaintext or in secret key the output change significantly (about half of the output).

If a cipher does not show desirable degree of avalanche effect then the cryptanalysts can guess the plaintext by analyzing the Cipertext. So they can be able to break the cipher.

$$\text{Avalenche effect} = \frac{\text{Hamming distance}}{\text{Block size}} * 100\%$$

Humming Distance:The Hamming Distance is a digit used to indicate the variation between two binary strings. It is a tiny section of a broader set of formulas used in information analysis. Specifically, Hamming's formulas allow computers to detect and correct error on their own [7].

3.2. Strict Avalanche Criterion

For symmetric key cryptographic algorithms Strict Avalanche Criterion is a wanted property. In block cipher context the SAC is said to be maintained by algorithms if, one bit complemented either in key or in plaintext causes a drastic change in ciphertext- about one half of the ciphertext. This SAC completely depends on algorithms confusion and diffusion property. In this AES symmetric key context SubBytes step, ShiftRows step and MixColumns step gives a desirable degree of confusion and diffusion.

4. SECURITY ANALYSIS OF EXISTING AES

4.1.AES-128

AES-128 algorithm uses 128 bit block of plaintext and 128 bit key. With the fastest Super Computer of this age it will take 3.19 x 1014 years to creak a key combination through brute force attack. So it is not possible not only for a human but also for a generation to break a key with checking all key combinations [8].

Case 1: Here the plaintext change by 1 byte in every experiment and the key is always constant.
Key (16 byte): 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f

Table 3. Avalanche Effect for fixed key 128 bit

No	Plaintext (Alphabet)	Ciphertext (Hex.)	Bit variance	Avalanche (%)
1	ABCDEFGHIJKLMNOP	9CDD85DE85B48BED892F02D8A5CBDACB	63	49.22
2	ABCDEFGHIJKLMNOQ	ACE7083761553A6B3A97BCB1740B176A		
3	ABCDEFGHIJKLMNOB	0026D76C52B61B9A76445035FD4D342B	69	53.91
4	ABCDEFGHIJKLMNOC	E930AC10030FA5DB617AF6DFA741ADE4		
5	ABCDEFGHIJKLMNOS	DA5D2C1E67818646AC2D955E0FAB4C3B	61	47.66
6	ABCDEFGHIJKLMNOR	7A6EEC02FCADA2FB323D672B3D2EF396		

Case 2: Here the plaintext is always constant and the key will be changed by 1 bit.
Input plaintext (16 bytes): ABCDEFGHIJKLMNOP

Table 4. Avalanche Effect for Fixed Plaintext but Variable Key

No	Key	Cipher text	Bit variance	Avalanche (%)
01	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 01	6DDDBB27CAB5B875FEEB 3B132AF00113	68	53.13
02	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 03	A65749D1BF1444BCEDB68 6837 C18E237		
03	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 00	0054396C46CC2330B334959 5A6529FCB	64	50.00
04	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 01	6DDDBB27CAB5B875FEEB 3B132AF00113		
05	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 06	D8B5B0EBF6787F53163B64 144393DEC8	66	51.56
06	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 07	7185F7D1451E8EE0530E676 A2F2D8560		

Table 5. SAC for AES-128

Case	Number of Samples	Number of samples satisfy SAC	Number of samples not satisfy SAC
Case 1	8112	4321	3791
Case 2	8112	4306	3806
Case 3	8112	4312	3800
Case 4	8112	4333	3779
Case 5	8112	4342	3770
Average		4322	3790

From table 3 and 4, we can say that AES-128 bit maintain a good degree of Claude Shannon's Confusion and diffusion property. For checking this property we deal with Avalanche effect. To determine Avalanche Effect in case 1 (table 3) we take fixed 128 bit key and different plaintext pair with difference of 1 bit and in case 2 (table 4) we take fixed plaintext and pair of keys with difference 1 bit. In each pair it shows a good degree of bit variance.

AES-128 also maintains a good degree of Strict Avalanche Criterion. Table 5 shows that among 8112 sample encryption, in average 4322 times it maintains SAC means for complementing 1 bit in input plaintext pair, it gives more or equal than 50% change in ciphertext in 4322 times.

4.2.AES-192

AES-128 algorithm uses 128 bit block of plaintext and 192 bit key. With the fastest Super Computer of this age it will take 5.88×10^{33} years to break a key combination through brute force attack. It is much bigger than AES-128.

Case 1: Here the plaintext change by 1 byte in every experiment and the key is always constant.
Key (24 byte): 00 01 02 03 04 05 06 07 08 09 0a 0b0c 0d 0e 0f 00 11 22 33 44 55 66 77

Table 6. Avalanche Effect for Fixed Key 192 Bit

No	Plaintext (Alphabet)	Ciphertext (Hex.)	Bit variance	Avalanche (%)
1	ABCDEFGHIJKLMNOP	61E3EBD043FD1D3C462637F071A0A7A5	61	47.56
2	ABCDEFGHIJKLMNOQ	50FD745C2B29B3D4431BE9C462A5D223		
3	ABCDEFGHIJKLMNOB	3147A88CEF8EA650A3A4912B49C25EEB	72	56.25
4	ABCDEFGHIJKLMNOC	7DF2DD5B5A9282260C62DEB4F7C1BD87		
5	ABCDEFGHIJKLMNOS	AA4B32F0A046700A41E2366C23BEFC4F	71	55.47
6	ABCDEFGHIJKLMNOR	0AB021AB56E6A9769DBC02E74A6DB198		

Case 2: Here the plaintext is always constant and the key will be changed by 1 bit.
Input plaintext (16 bytes): ABCDEFGHIJKLMNOP

Table 7. Avalanche Effect for Fixed Plaintext but Variable Key

No	Key	Cipher text	Bit variance	Avalanche (%)
1	000102030405060708090a0b0c0d0e010011223344556677	B77187B4A3DCE3162925A05A6EE4ED96	59	46.09
2	000102030405060708090a0b0c0d0e010011223344556677	F6717C9D366309BA238F831642AB4FE2		
3	000102030405060708090a0b0c0d0e010011223344556677	83939EA12E5AE52966557CBD34BED2E8	67	52.34
4	000102030405060708090a0b0c0d0e010011223344556677	B77187B4A3DCE3162925A05A6EE4ED96		
5	000102030405060708090a0b0c0d0e010011223344556677	D07C2AA15BC600399144942A6AEADFEC	65	50.78
6	000102030405060708090a0b0c0d0e010011223344556677	BDA92F2024FC271A3ECCE720EC24316B		

From table 6 and7, we can say that AES-192 bit also maintain a good degree of Claude Shannon's Confusion and diffusion property. To determine Avalanche Effect in case 1 (table 6) we take fixed 192 bit key and different plaintext pair with difference of 1 bit and in case 2 (table 7) we take fixed plaintext and pair of keys with difference 1 bit. In each pair it shows a good degree of bit variance. On an average for flipping 1 bit the ciphertext change about 50%.

Table 8. SAC for AES-192

Case	Number of Samples	Number of samples satisfying SAC	Number of samples not satisfying SAC
Case 1	8112	4352	3760
Case 2	8112	4309	3803
Case 3	8112	4321	3791
Case 4	8112	4365	3747
Case 5	8112	4276	3836
Average		4324.6	3787.4

AES-192 also maintains a good degree of Strict Avalanche Criterion. Table 8shows that among 8112 sample encryption, in average 4324 times it maintains SAC. It means for complementing 1 bit in input plaintext pair, it gives more or equal than 50% change in ciphertext in 4324 times.

4.4.AES-256

AES-256 algorithm uses 128 bit block of plaintext and 256 bit key. With the fastest Super Computer of this age it will take 1.0844 x 10^{53} years to creak a key combination through brute force attack. So it is not possible not only for a human but also for a generation to break a key with checking all key combinations.

Case 1: Here the plaintext change by 1 byte in every experiment and the key is always constant.
Key (32 byte): 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 00 11 22 33 44 55 66 7788 99 aa bb cc dd ee ff

Table 9. Avalanche Effect for Fixed Key 256 Bit

No	Plaintext (Alphabet)	Ciphertext (Hex.)	Bit variance	Avalanche (%)
1	ABCDEFGHIJKLMNOP	A6E6D3062B8F19F3D9B5 D6FE4A37B121	60	46.67
2	ABCDEFGHIJKLMNOQ	99200F5E3B07A78142E6F B7E8EF2ADC4		
3	ABCDEFGHIJKLMNOB	CFFFE86126B1A755D7E8 39702D5F2274	68	53.15
4	ABCDEFGHIJKLMNOC	A3C073EDE91BBC744AE 0FBC3D7511DFB		
5	ABCDEFGHIJKLMNOS	27CF10396B33E1E299B00 C43D4A9AAAE	53	41.40
6	ABCDEFGHIJKLMNOR	50EA30406AD10DE79999 6AEDFC679924		

Case 2: Here the plaintext is always constant and the key will be changed by 1 bit.
Input plaintext (16 bytes): ABCDEFGHIJKLMNOP

Table 10. Avalanche Effect for Fixed Plaintext but Variable Key

No	Key	Cipher text	Bit variance	Avalanche (%)
1	000102030405060708090a0b0c0d0e01 00112233445566778899aabbccddeeff	E8A178B770C8C17C AB13CE2317471D7 C	68	53.13
2	000102030405060708090a0b0c0d0e01 00112233445566778899aabbccddeeff	4775A73EC2B69610 DC118C7E62723FBF		
3	000102030405060708090a0b0c0d0e01 00112233445566778899aabbccddeeff	6D8A81E21A9BC04 886CF72BA66DFFE 37	63	49.21
4	000102030405060708090a0b0c0d0e01 00112233445566778899aabbccddeeff	E8A178B770C8C17C AB13CE2317471D7 C		
5	000102030405060708090a0b0c0d0e01 00112233445566778899aabbccddeeff	154ED6F672645C88 6997D9087C9D28C5	66	51.56
6	000102030405060708090a0b0c0d0e01 00112233445566778899aabbccddeeff	2CEB0EEBECFB5E5 166FD7B46428B5FD E		

From table 9 and 10, we can say that AES-128 bit maintain a good degree of Claude Shannon's Confusion and diffusion property. To determine Avalanche Effect in case 1 (table 9)we take fixed

128 bit key and different plaintext pair with difference of 1 bit and in case 2 (table 10) we take fixed plaintext and pair of keys with difference 1 bit. In each pair it shows a good degree of bit variance. With fixed plaintext and variable key almost all the time it shows avalanche affect more than 50%.

Table 11. SAC for AES-256

Case	Number of Samples	Number of samples satisfy SAC	Number of samples not satisfy SAC
Case 1	8112	4388	3724
Case 2	8112	4311	3801
Case 3	8112	4317	3795
Case 4	8112	4495	3617
Case 5	8112	4375	3737
Average		4377.2	3734.8

AES-256 also maintains a good degree of Strict Avalanche Criterion. Table 11 shows that among 8112 sample encryption, in average 4377 times it maintains SAC means for complementing 1 bit in input plaintext pair, it gives more or equal than 50% change in ciphertext in 4377 times.

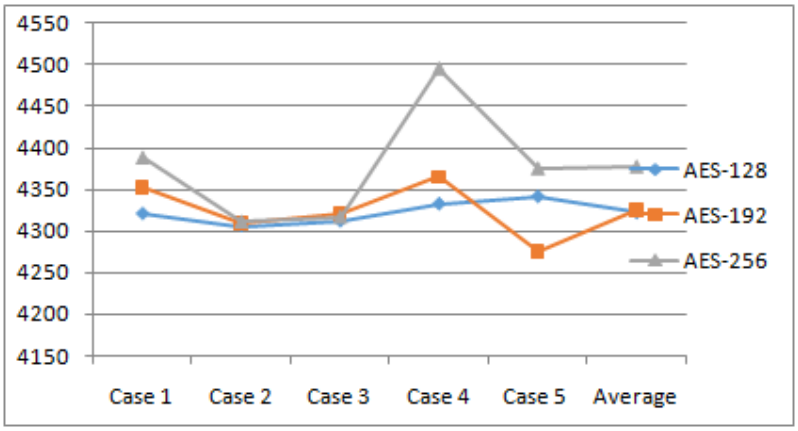

Figure 5. SAC Property of AES

5. PROPOSED SYSTEM FOR AES

5.1.Changes to Existing System

AES is already a secured algorithm beyond all cryptanalysis. For cryptanalysis, hackers always try to find the cipher key by which the cipher text can be decrypt. In theory, brute force is the most common cryptanalysis, which can be used against all cryptographic algorithms. In brute force attack, hackers search the cipher key among all possible combination of keys. They compute every possible combination of keys and perform a trail decryption for testing if it is the accurate key. Now the question is that, how long time is needed for brute force to find the actual key? The time for brute force attack depends on the key size. If the key size is small, it can be found very quickly. But if the key size is longer, then it may be take very long time to find the actual key[8].

To increase the brute force attack time in our propose plan of new AES, we increase the key size by 8 bits. That means the existing key size is extended from 128 to 136, 192 to 200 and 256 to 264. This additional 8 bits are generated by a user defined function named getRandKey for encryption and are stored secretly for further use in decryption. The 8 bits key is used in the time of getSBoxValue execution. In getSBoxValue function, the 8 bit random key is Xor'ed the substituted s-box value during the key expansion and the execution of SubBytes step for each round. As a result, the key expansion time increases significantly which makes the brute force attack more time consuming. On the other hand, the additional key also increases the time security more than 2^8 times. To implement our propose plan we have to change the existing AES both for encryption and decryption.

5.2.Encryption

5.2.1getRandKey

The getRandKey is a user defined function used in encryption algorithm for our proposed plan in addition with the existing AES. This function is used to generate 8 bits random key. As getRandKey is a user defined function, the consumer can use any kind of random generator to generate the 8 bits random key. The user must have to generate the key before key expansion in main algorithm and store the key for decryption.

5.2.2.getSBoxValue

In existing AES, getSBoxValue is a function to substitute a value with a corresponding value in s-box. This function is used during the key expansion and the execution of SubBytes in each round for encryption algorithm. In our propose plan, every time the corresponding s-box value are Xor'ed with the 8 bits key.

5.3.Decryption

The cipher text generated by our proposed algorithm can be decrypted by usual AES decryption algorithm using the additional 8 bits key which was generated during encryption algorithm. In proposed AES decryption algorithm the 8 bits key is Xor'ed with each cipher byte before substituting with s-box value and all other task in decryption processes are remain unchanged.

6. SECURITY ANALYSIS OF PROPOSED AES

In section3, we have discussed about security measurement criteria for AES cryptosystem. Now, we will measure the security for all 128, 192 & 256 bits proposed AES based on three criteria.

6.1 128 Bit Proposed AES

6.1.1.Time Security

In section3, we have calculated that, brute force attack must check maximum $3.403x10^{38}$key combinations for existing AES-128 and it needs almost 3.19×10^{14}years to find the key with the fastest Super Computer of this age. In our proposed AES-128,[12][7] the plaintext block size is 128, key size is 128 and additional random key size is 8. For this additional 8 bits, brute force attack has to check maximum $3.403+E^{38} \times 2^8$ (8.712×10^{40})key combinations and it needs maximum $3.19+E^{14} \times 2^8$ (8.165×10^{16}) years to crack the proposed AES-128 with the fastest

Super Computer of this age. So, it is not possible for human being to check all the key combination.

6.1.2.Avalanche Effect

To compute the avalanche effect of proposed AES-128, we consider two case[18][19]
Case 1: Here, the plaintext changes by 1 bit in every experiment, the 128 bit key is always constant and the additional 8bit key is random.

Key (16 byte): 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Table 12. Avalanche Effect for Fixed 128 Bit Key and Variable Input Block

No	Plaintext (Alphabet)	Ciphertext (Hex.)	Bit variance	Avalanche (%)
1	ABCDEFGHIJKLMAAB	AB008578C77D2A09C0D9963 631CD158B	63	49.22
2	ABCDEFGHIJKLMAAC	2CA28FF350D43C76EA63009 0F6BD5CB1		
3	ABCDEFGHIJKLMAAP	393A42E7681CA8659B48DA2 022771CD7	72	56.25
4	ABCDEFGHIJKLMAAQ	FF59F19913AD598154775653 87D36494		
5	ABCDEFGHIJKLMABT	8E61F8C978621C3397120176 FEEB1B65	73	57.03
6	ABCDEFGHIJKLMABU	332B18222296ABEABC2F90 A581C7AA59		

Case 2: In this case, the plaintext is always constant; the key changes by 1 bit and the additional 8bit key is random.

Input plaintext (16 bytes): 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

Table 13. Avalanche Effect for Fixed Plaintext but Variable Key

No	Key	Cipher text	Bit variance	Avalanche (%)
01	ABCDEFGHIJKLMAAB	0FBF2E621156D6D4388304 C11496166C	70	54.69
02	ABCDEFGHIJKLMAAC	332AAF8DEF11A6F2B3D49 5341E5EECD3		
03	ABCDEFGHIJKLMAAR	8B84E4D40048BD63E6EB0F 712EA825C2	61	47.66
04	ABCDEFGHIJKLMAAS	A05F3A439058794D33548D B7B5AE2EE6		
05	ABCDEFGHIJKLMAEJ	FB8A1570B3A4400212C958 2384DB3FE6	73	57.03
06	ABCDEFGHIJKLMAEK	CE7228908E0F971E832F1FE 963B443D5		

Table 12 shows that, single bit variance in input plaintext shows a large number of bit variance in output. Again table 13 also shows that, single bit variance in 128 bit key shows a large number of bit variance in output. After all from both table we can say that, our proposed AES-128 maintains a good degree of Claude Shannon's Confusion and Diffusion property.

6.2.4.Strict Avalanche Criterion

For measuring Strict Avalanche criteria, we analyzed five experiments. Here the 128 bits key is fixed and the additional 8 bits key is random.

Table 14. SAC for Proposed AES-128

Exp. No	Number of Samples	Total satisfying SAC	Satisfying SAC (%)
1	8112	4353	53.66
02	8112	4361	53.76
03	8112	4333	53.42
04	8112	4366	53.82
05	8112	4322	53.27
Average		4347	53.587

Table 14 shows that, in five experiments for 8112 sample encryption, average 4347 times the proposed AES-128 maintains the SAC condition. That means for single bit variance in input plaintext, bit variance in chipper text is more than 50% for average 4347 times.

6.2 192 Bits Proposed AES

6.2.1.Time Security

For existing AES-192 we have calculated in section3 that, brute force attack has to check maximum 6.278 x 10^{57} key combinations to find the key and it needs almost 5.88 x 10^{33} years to crack AES-192 [1]with the fastest Super Computer of this age. In our proposed AES-192, the plaintext block size is 128, key size is 192 and additional random key size is 8. For this additional 8 bits, brute force attack has to check maximum6.278+E^{57} x 2^{8} (1.607 x 10^{60}) key combinations to find the key and it needs maximum 5.88+E^{33} x 2^{8} (1.505 x 10^{36}) years to crack the proposed AES-192 with the fastest Super Computer of this age. So, it is not possible for human being to check all the key combination.

6.2.2.Avalanche Effect

To compute the avalanche effect of proposed AES-192, we consider two cases.

Case 1: Here, the plaintext changes by 1 bit in every experiment, the 192 bit key is always fixed and the additional 8 bit key is random.

Key (24 byte): 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F FF EE DD CC BBAA 99 88

Table 15. Avalanche Effect for Fixed 192 Bit Key and Variable Input Block

No	Plaintext (Alphabet)	Cipher text (Hex.)	Bit variance	Avalanche (%)
1	ABCDEFGHIJKLMAAH	967F4C15877D78715A3570 D7056E6B6F	61	47.66
2	ABCDEFGHIJKLMAAI	41DAC48B55ACE7D2A473 7BF31224437D		
3	ABCDEFGHIJKLMAAR	E655CB7A0438DC3E9302A D6B92C0CC6D	68	53.13

4	ABCDEFGHIJKLMAAS	554F961504452EE518004E AA426E55B2		
5	ABCDEFGHIJKLMAFL	EDCEBC097327B076D0F28 8197FDA1449	72	56.25
6	ABCDEFGHIJKLMAFM	84C9228E9EF205E0DE5B6 F6EB18FF495		

Case 2: In this case, the plaintext is always fixed; the key changes by 1 bit and the additional 8bit key is random.

Input plaintext (16 bytes): 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

Table 16. Avalanche Effect for Fixed Plaintext but Variable Key

No	Key	Cipher text	Bit variance	Avalanche (%)
01	ABCDEFGHIJKLMNOPQR STUZZX	50F9896E4992F2039F7604B E6C3BEBAC	83	64.84
02	ABCDEFGHIJKLMNOPQR STUZZY	2F10071C3D05EDBEA15DC 9CB16989845		
03	ABCDEFGHIJKLMNOPQR STUZZH	DE8C6CB72C7D3F43430131 9F23A42FF3	77	60.16
04	ABCDEFGHIJKLMNOPQR STUZZI	A58B071B4916A7BFFB4F2C 71F510F4B5		
05	ABCDEFGHIJKLMNOPQR STUZYT	B74FA6657358FAA2A2D4E8 4E123D68E3	67	52.34
06	ABCDEFGHIJKLMNOPQR STUZYU	D0FF63D95A499716C187F11 C71C8795A		

Table 15 shows that, single bit variance in input plaintext shows a large number of bit variance in output cipher text. Again, table 16 also shows that, single bit variance in 192 bits key shows a large number of bit variance in output. After all, from both table we can say that, our proposed AES-192 maintains a good degree of Claude Shannon's Confusion and Diffusion property.

6.2.3.Strict Avalanche Criterion

For measuring Strict Avalanche criteria, we analyzed five experiments. Here the 192 bits key is fixed and the additional 8 bits key is random.

Table 17. SAC for Proposed AES-192

Experiment No	Number of Samples	Total satisfying SAC	Satisfying SAC (%)
01	8112	4385	54.06
02	8112	4329	53.37
03	8112	4410	54.36
04	8112	4372	53.90
05	8112	4348	53.60
Average		4368.8	53.858

Table 17 shows that, in five experiments for 8112 sample encryption, average 4368.8 times the proposed AES-192 maintains the SAC condition. That means for single bit variance in input plaintext, bit variance in chipper text is more than 50% for average 4368.8 times.

6.3 256 Bit Proposed AES

6.3.1 Time Security

For existing AES-256 brute force attack checks maximum 1.158×10^{77} key combinations to find the key and it needs almost 5.88×10^{33} years to crack AES-256 with the fastest Super Computer of this age. In our proposed AES-256, the plaintext block size is 128, key size is 256 and additional random key size is 8. For this additional 8 bits, brute force attack has to check maximum $1.158+E^{77} \times 2^8$ (2.965×10^{79}) key combinations to find the key and it needs maximum $1.0844+E^{53} \times 2^8$ (2.776×10^{55}) years to crack the proposed AES-256[15][12]with the fastest Super Computer of this age. So, it is not possible for human being to check all the key combinations.

6.3.2 Avalanche Effect

To compute the avalanche effect of proposed AES-256, we consider two cases.

Case 1: Here, the plaintext changes by 1 bit in every experiment, the 256 bit key is always fixed and the additional 8 bits key is random.

Key (32 byte): 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F FF EE DD CC BB AA 99 88 77 66 55 44 33 22 11 2A

Table 18. Avalanche Effect for Fixed 256 Bit Key and Variable Input Block

No	Plaintext (Alphabet)	Cipher text (Hex.)	Bit variance	Avalanche (%)
1	ABCDEFGHIJKLMYWJ	23EE09863ECF2D1756CA 4F940D183CD0	78	60.94
2	ABCDEFGHIJKLMYWK	DC5CFEDE24DA768ACE2 DB1A556E3C802		
3	ABCDEFGHIJKLMYVF	AE22A21F677E4330D14E B22667351327	71	55.47
4	ABCDEFGHIJKLMYVG	5B3536BD332118FF8BB8 B8DB16F59DFA		
5	ABCDEFGHIJKLMXVL	32CE61C5C6A549C9ABB4 51EAA17CAADB	67	52.34
6	ABCDEFGHIJKLMXVM	DCAE188970EDD3AF1445 9304135AA5BE		

Case 2: In this case, the plaintext is always fixed; the 256 bit key changes by 1 bit and the additional 8 bits key is random.

Input plaintext (16 bytes): 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

Table 19. Avalanche Effect for Fixed Plaintext but Variable Key

No	Key	Cipher text	Bit variance	Avalanche (%)
01	1234ABCDEFGHIJKLMNOP QRSTUVWRXP	F74AEE57EFE17B4B35EA 6439665DFD32	71	55.47
02	1234ABCDEFGHIJKLMNOP QRSTUVWRXQ	CCC3E46A61368F5457F57 84343EF4F85		
03	1234ABCDEFGHIJKLMNOP	A9889A3DBC7A893754541	77	60.16

	QRSTUVWPSD	CBD00D0BDCB		
04	1234ABCDEFGHIJKLMNOP QRSTUVWPSE	2E7909A6D388B6AD3E850 258E269AEB5		
05	1234ABCDEFGHIJKLMNOP QRSTUVWLVB	2266294E8EDD8C597D621 620FEEC747D	77	60.16
06	1234ABCDEFGHIJKLMNOP QRSTUVWLVC	912DC8BF601E5A0E2E55C B85D5C02FAB		

Table 18 shows that, single bit variance in input plaintext shows a large number of bit variance in output cipher text. Again, table 19 also shows that, single bit variance in 256 bits key shows a large number of bit variance in output. After all, from both table we can say that, our proposed AES-256 maintains a good degree of Claude Shannon's Confusion and Diffusion property.

6.3.1 Strict Avalanche Criterion

For measuring Strict Avalanche criteria, we analyzed five experiments. Here the 256 bits key is fixed and the additional 8 bits key is random.

Table 20. SAC for Proposed AES-256

Experiment No	Number of Samples	Total satisfying SAC	Satisfying SAC (%)
01	8112	4359	53.74
02	8112	4315	53.19
03	8112	4424	54.54
04	8112	4387	54.08
05	8112	4444	54.78
Average		4385.8	54.066

Table20 shows that, in five experiments for 8112 sample encryption, average 4385.8 times the proposed AES-256 maintains the SAC condition. That means for single bit variance in input plaintext, bit variance in chipper text is more than 50% for average 4385.8 times.

7. SECURITY COMPARISONS OF PROPOSED AES WITH EXISTING SYSTEM

7.1 Time Security

The comparison between existing and proposed AES in basis of time security is given in table 21.

Table 21. Time Security Comparison between Existing & Proposed AES System

Key Size	Existing System		Proposed System	
	Max Possible combinations	Time Needed to Crack(Years)	Max Possible combinations	Time Needed to Crack(Years)
128	3.403×10^{38}	3.19×10^{14}	8.712×10^{40}	8.165×10^{16}
192	6.278×10^{57}	5.88×10^{33}	1.607×10^{60}	1.505×10^{36}
256	1.158×10^{77}	1.0844×10^{53}	2.965×10^{79}	$2.776 10^{55}$

7.2 Avalanche Effect

In existing system, if the key (128, 192 or 256) and input block are fixed then the avalanche effect is constant. But in proposed plan, although the key (128, 192 or 256) and input block are fixed, the 8 bit key is random with each execution. So the avalanche effect always varies with every execution.

To compare Avalanche effect criteria between existing & proposed plan, we did three experiments for proposed plan and a single experiment for existing system. In every experiment 8112 sample inputs were taken. For every input, we computed the avalanche effect and took the average of all 8112 inputs. The total result is enlisted in table 22.

Table 22. Avalanche Effect Comparison between Existing & Proposed AES System

Key Size	Existing System Average Avalanche Effect (%)	Proposed system Average Avalanche Effect (%)		
		Exp No. 01	Exp No. 02	Exp No. 03
128	49.977657	49.950883	49.948379	49.926132
192	50.036308	49.979294	49.947031	49.984591
256	50.042664	50.040835	50.087929	50.071749

7.3 Strict Avalanche Criterion

To compare strict avalanche effect between existing & proposed system, we did five experiments. In each experiment there were 8112 sample inputs. After completing those experiments, we have enlisted the average result in table 23

Table 23. SAC Comparison between Existing & Proposed AES System

Key Size	Satisfying SAC for Existing System		Satisfying SAC for Proposed System	
	Average of five Experiment	Percentage of five experiment	Average of five Experiment	Percentage of five experiment
128	4322	53.279	4347	53.587
192	4324.6	53.311	4368.8	53.858
256	4377.2	53.96	4385.8	54.66

8. RESULT & CONCLUSION

We have studied the existing Advanced Encryption Standard and its implementation. We have also analyzed the security of existing AES algorithm in basis of time security, avalanche effect, and strict avalanche effect. We conclude that AES is one of the best secured algorithms at present time. Although, historically, brute force attack can be used against all cryptographic algorithms.
In our work, we have proposed a new plan and enhanced the security by XORing a new 8 bit key in key expansion and each round of existing system. We have also analyzed the security of our proposed plan in basis of those three criteria. Finally, we have found that the time security of the proposed plan increases by 256 times compared to the existing system. The avalanche effect always fluctuates with each execution while the avalanche effect in existing system is always fixed and the strict avalanche effect of the proposed system is greater than the existing system for all 128, 192 and 256 key sizes.

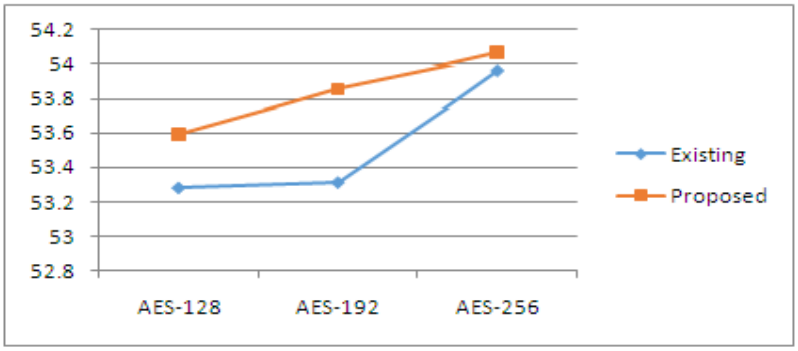

Figure 8. SAC Comparisons between Existing and Proposed AES

REFERENCES

[1] Guy-Armand Yandji, Lui Lian Hao, Amir-Eddine Youssouf, Jules Ehoussou, "RESEARCH ON A NORMAL FILE ENCRYPTION AND DECRYPTION" in proceedings of IEEE 2011.

[2] Hyubgun Lee, Kyounghwa Lee, Yongtae Shin, "AES Implementation and Performance Evaluationon 8-bit Microcontrollers", International Journal of Computer Science and Information Security,Vol. 6 No. 1, 2009

[3] "Specification for the ADVANCED ENCRYPTION STANDARD (AES)", Federal Information Processing Standards Publication 197 November 26, 2001

[4] Saberi, I. Shojaie, B. ; Salleh, M. "Enhanced Key Expansion for AES-256 by using Even-Odd method", Research and Innovation in Information Systems (ICRIIS), 23-24 Nov. 2011

[5] Liam Keliher ,"Substitution-Permutation Network Cryptosystems Using Key-Dependent Boxes", http://www.researchgate.net/publication/2822741, ARTICLE • NOVEMBER 1997

[6] Krishnamurthy G N and V Ramaswamy, "Making AES Stronger: AES with Key Dependent S-Box." International Journal of Computer Science and Network Security, VOL.8 No.9, September 2008

[7] Mohan H. S. and A Raji Reddy, " Performance Analysis of AES and MARS Encryption Algorithms", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011

[8] Manisha S. Mahindrakar' "Evaluation of Blowfish Algorithm based on Avalanche Effect", International Journal of Innovations in Engineering and Technology (IJIET), Vol. 4 Issue 1 June 2014

[9] Akash Kumar Mandal1, Mrs. Archana Tiwari, "Analysis of Avalanche Effect in Plaintext of DES using Binary Codes", International Journal of Security, Privacy and Trust Management, Volume 1, Issue 3, September – October 2012

[10] SriramRamanujam and MarimuthuKaruppiah, "Designing an algorithm with high Avalanche Effect", International Journal of Computer Science and Network Security, VOL.11 No.1, January 2011

[11] K.Anchugam and M.Tamilselvi "New Data Encryption Standard Algorithm" , International Journal of Computer Science and Network Security, VOL.13 No.4, April 2013

[12] M.Abirami, S. Chellaganeshavalli, "Performance Analysis of AES and Blowfish Encryption Algorithm", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, Issue 11, November 2013

[13] AbdulkarimAmerShtewi, BahaaEldin M. Hasan and Abd El Fatah .A. Hegazy," An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems", International Journal of Computer Science and Network Security, VOL.10 No.2, February 2010

[14] Nidhi Singhal and J.P.S.Raina, Comparative Analysis of AES and RC4 Algorithms for Better Utilization, International Journal of Computer Trends and Technology- July to Aug Issue 2011

[15] M.Abirami, S. Chellaganeshavalli, "Performance Analysis of AES and Blowfish Encryption Algorithm", International Journal of Innovative Research in Science,Engineering and Technology, Vol. 2, Issue 11, November 2013

[16] Chandra Prakash Dewangan,Shashikant Agrawal, A Novel Approach to Improve Avalanche Effect of AES Algorithm, International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 8, October 2012

[17] Amish Kumar , Mrs. Namita Tiwari, "EFFECTIVE IMPLEMENTATION AND AVALANCHE EFFECT OF AES", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 3/4, August 2012

[18] Akash Kumar Mandal, Mrs. Archana Tiwari, "Analysis of Avalanche Effect in Plaintex of DES using Binary Codes", International Journal of Security, Privacy and Trust Management (IJSPTM), Volume 1, Issue 3, September – October 2012
[19] Jayant P. Bhoge, Dr. Prashant N. Chatur," Avalanche Effect of AES Algorithm", International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014, 3101 – 3103
[20] Opala, Omondi John; Rahman, Shawon; and Alelaiwi, Abdulhameed; "The Influence of Information Security on the Adoption of Cloud computing: An Exploratory Analysis", International Journal of Computer Networks & Communications (IJCNC), Vol.7, No.4, July 2015
[21] Rader, A., Marc and Rahman, Syed (Shawon); "Exploring Historical and Emerging Phishing Techniques and Mitigating the Associated Security Risks"; International Journal of Network Security & Its Applications (IJNSA), ISSN:0974-9330(online); 0975-2307
[22] Opala, John, Omondi; Rahman, Shawon and Alelaiwi, Abdulhameed ; "An Analysis on the Factors Influencing Managers' Decision to Adopt of Cloud Computing"; " Handbook of Research on Architectural Trends in Service-Driven Computing" IGI Global in 2014,DOI: 10.4018/978-1-4666-6178-3

Authors

Abdullah Al- Mamun: Abdullah Al- Mamun is doing MSc in Computer Science & Engineering in Jessore University of Science & Technology. He earned his graduation degree in CSE from same university in 2015. His research focus is on information security, cloud technology and specially on encryption technology. Mamun has two years of work experience in the field of web application development.

Dr. Shawon Rahman: Dr. Shawon S. M. Rahman is an Associate Professor in the Department of Computer Science at the Majmaah University, Majmaah, KSA. Dr. Rahman's research interests includeInformation Assurance and Security, Software Engineering education, Software Testing & QA, Cloud Computing, Mobile Application Development, and Web Accessibility. He has published over 100 peer-reviewed articles and is a member of many professional organizations including IEEE, ACM, ASEE, ASQ, ISACA, and UPE.

Tanvir Ahmed Shaon: Tanvir Ahmed Shaon has earned his master's degree in Computer Science and Engineering from Military institute of science and technology. His research focus is on Ad-hoc network security. He also holds an BSc in Computer Science and Engineering. Shaon has two years' work experience in the field of web technology

Md Alam Hossain: Md. Alam Hossain is working as an Assistant Professor at the department of Computer Science & Engineering in Jessore University of Science & Technology (JUST), Jessore, Bangladesh. Prior to that, he joined as Lecturer at the same department. He completed his B.Sc and M.Sc (Thesis) in Computer Science & Engineering from Islamic University, Kushtia, Bangladesh. Currently he is pursuing PhD on Cloud Computing Security. His research interest fields are Cloud Computing, Cloud Computing Architecture, Cloud Computing Security Issues, Cloud Computing Application Services and Quality, Cyber Security, Banking Solutions Security, Network Security, Digital Forensic Science, Steganography, Information Security, Internet Security.