https://doi.org/10.46335/IJIES.2025.10.7.4 e-ISSN: 2456-3463
Vol. 10, No. 7, 2025, PP. 16-21
International Journal of Innovations in Engineering and Science, www.ijies.net

A Cryptographic Enhancement for Strengthened AES Resilience

Sunil Kishor Khode[1], Dr. Manish P. Deshmukh[2]

[1]*Research Scholar, : 0009-0001-1705-6460,*
SSBT's COET, Bambhori, Jalgon, India, Pin-425001,
[2]*Professor & Head, E & TC Engg. Dept., : 0009-0001-2557-2596*
SSBT's COET, Bambhori, Jalgaon, India, Pin-425001, rushimd@yahoo.com

Email of corrsponding Author : ***khodesunil@gmail.com***

***Received on**: 7May,2025* ***Revised on**: 08 June,2025* ***Published on**: 10 June,2025*

***Abstract**– AES is a widely used encryption technique for securing digital data. This study presents a new method aimed at improving the avalanche effect in the AES algorithm., which is a critical factor for ensuring data security. However, enhancing its security further remains a topic of interest. This paper explores an optimized method to improve the avalanche effect in AES by incorporating modifications in the S-Box transformation. The proposed approach demonstrates an increased diffusion rate, leading to improved security against cryptanalysis. Comparative analysis with conventional AES highlights the advantages of the modified model.*

***Keywords—**Cryptography, AES, Avalanche effect, Add round Key*

INTRODUCTION

Security concerns in digital communication have led to extensive research in cryptographic algorithms. AES, as a symmetric block cipher, is known for its efficiency and security. The avalanche effect, a crucial property in cryptographic systems, ensures that minor changes in input lead to significant alterations in output. This study aims to enhance this effect by refining the S-Box structure in AES.

Previous studies have underscored the significance of the avalanche effect in strengthening cryptographic algorithms. Research indicates that enhancing substitution and permutation processes can lead to better security outcomes. Notably, modifications in S-Box designs have been a focal point for achieving improved diffusion characteristics. This paper builds upon these foundational insights, proposing a refined method for enhancing AES's resistance to differential and linear cryptanalysis. The S-Box, a nonlinear substitution stage, plays a pivotal role in enhancing security. In the current digital era, transmitting plain (readable) data over the internet poses significant security risks due to potential intrusions by unauthorized entities aiming to access sensitive information. Such critical data may include e-banking credentials, confidential emails, or private conversations on social media platforms. To safeguard this information, various security measures are employed, with cryptography being one of the most essential techniques. Cryptography plays a key role in protecting sensitive information by transforming readable data into an unintelligible format known as ciphertext through a process called encryption. To make the data understandable again, the ciphertext is converted back into its original form using decryption. This process takes place at the receiver's end and effectively reverses encryption. A cryptosystem refers to the overall setup that supports both encryption and decryption functions. Figure 1 illustrates the basic concept of how these processes are carried out. [1].

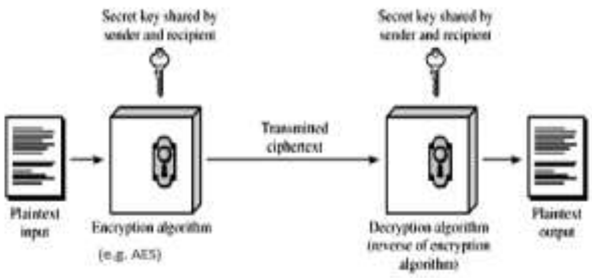

Fig.1 AES Encryption system

I. A Concise Overview of Cryptography:

Cryptography aims to achieve several core objectives as follows:

, one of which is confidentiality—ensuring that information is accessible only to those with the proper authorization.which are explained

•**Confidentiality:** It ensures that information is accessible only to those with the proper authorization, which are explained

• **Integrity:** Guarantees that the data remains unaltered during its transmission from sender to receiver.

•**Authentication:** Verifies the origin of the data and confirms the identity of the sender, helping to prevent disputes regarding the data's origin or delivery path.

•**Non-repudiation:** Ensures that the sender cannot deny having sent the information.. Cryptographic techniques are broadly categorized based on the type of security keys used, primarily into **symmetric** and **asymmetric** encryption. These techniques are discussed in the following sections.

A. Symmetric (Private Key) Encryption

In symmetric key encryption, the same secret key is shared between the sender and the receiver for both encrypting and decrypting the information must agree on the encryption algorithm before initiating data exchange. They also share a single secret key used for both encrypting and decrypting the data. Once the algorithm and key are agreed upon, the sender transmits the encrypted data along with the key. The receiver applies the identical secret key to convert the encrypted data back to its original form. A key challenge in this approach is securely sharing the secret key. If unauthorized entities discover the key, the confidentiality of the data is compromised. Additionally, effective key management becomes more complex as the number of users increases. For instance, if n participants are communicating, a total of $n(n - 1)/2$ unique secret keys are required to maintain secure communication between all parties.

B. Asymmetric (Public Key) Encryption

Asymmetric encryption uses two separate keys: one public and one private. The public key is available to anyone, while the private key is kept secure by its owner. To begin communication, both parties share their public keys. When transmitting data, the sender encrypts it using the recipient's public key, allowing only the recipient—who holds the matching private key—to decode the message. This method effectively addresses key management challenges, as there is no need to share private keys. However, asymmetric encryption requires more computational resources and is significantly slower—approximately 1,000 times slower—than symmetric encryption. This limitation makes it less efficient for devices with limited processing power, such as mobile phones or tablets.

To overcome this challenge, a hybrid encryption approach is often adopted. In this method, asymmetric encryption is used solely for securely exchanging the secret key, while symmetric encryption handles the actual data transfer, optimizing both security and performance.

C. Hashing

Hashing in cryptography plays a vital role in verifying that data has not been altered and confirming the identity of its source. It involves applying a hash function to the input data, generating a fixed-length output known as a hash or digest. This output serves as a unique identifier, much like a digital fingerprint of the original content.Upon receiving the data, the recipient can apply the same hash function to verify the integrity of the message. If the computed hash matches the original hash value, it confirms that the data has not been altered during transmission. Any mismatch indicates potential tampering or corruption.

II. Internal structure of AES

AES is a symmetric block cipher that processes data in 128-bit blocks and allows key lengths of 128, 192, or 256 bits. These key sizes were selected to align with the security criteria outlined by NIST during the development of the standard. The number of encryption rounds carried out by the algorithm depends on the length of the key, as detailed in Table 1 [2].

Table 1: Key length and number of rounds of AES

Block Size (Bits)	Key Length (Bits)	No. of Round
128	128	10
128	192	12
128	256	14

https://doi.org/10.46335/IJIES.2025.10.7.4 e-ISSN: 2456-3463
Vol. 10, No. 7, 2025, PP. 16-21

Key Addition Layer: At this stage, a 128-bit subkey is derived from the original key through a key scheduling method. This subkey is then merged with the current data state using the XOR operation.

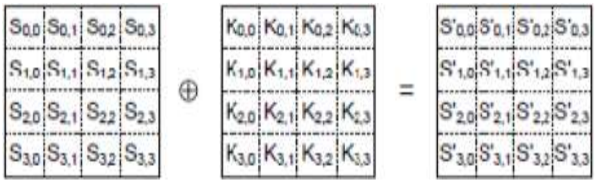

Fig. 2 Add round Key operation

1.1 Confusion Layer:

The Confusion Layer enhances security by altering the relationship between the plaintext and the ciphertext**.** It achieves this by substituting elements within the state table, effectively transforming the original content into a more complex and less predictable form.

Byte Substitution layer (S-Box):

In the Byte Substitution phase, every byte in the data block is replaced using a predefined lookup table called the S-Box. This non-linear substitution disrupts patterns between the original data and the encrypted output, enhancing resistance to various cryptographic attacks [2].

X \ Y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	1	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	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
4	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	2	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	6	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	8
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	3	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

Fig. 3 S- Box

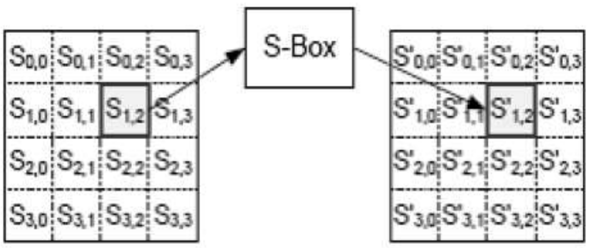

Fig.4 Byte Substitution Process

1.3 Diffusion Layer: The Diffusion Layer ensures that the influence of each input bit is spread across multiple output bits, enhancing the complexity of the cipher. This layer consists of two sub-layers, both performing linear transformations to achieve diffusion:

Shift Rows layer: In this stage, each row of the state matrix is rotated by a certain number of positions in a circular manner.This step helps in dispersing the data across columns, increasing the diffusion effect and contributing to the overall strength of the encryption This defines the method used to rotate the rows, as illustrated in Figure 5. based on the output of the previous layer.

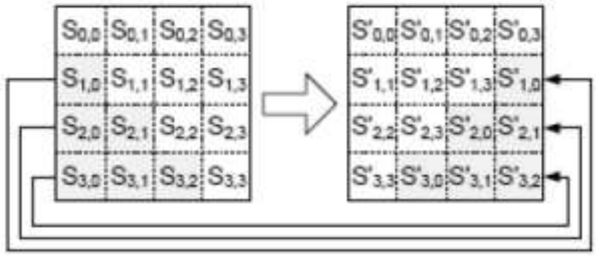

Fig.5 Shift Row Process

Mix Column layer: In the Mix Columns stage, each column of four bytes from the state is considered as a vector and is transformed through multiplication with a fixed 4×4 matrix composed of constant values. This transformation enhances the diffusion property by ensuring that each byte of a column affects all four bytes of the resulting column. The matrix used for this operation is illustrated in Fig. 6.

The overall AES encryption process is depicted in Fig. 7**.** Notably, the final round of AES excludes the Mix Columns **step**, which contributes to the cipher's strength and complexity.

Decryption reverses the encryption steps by applying operations like inverse substitution, inverse row rotation, and inverse column transformation to restore the original plaintext.

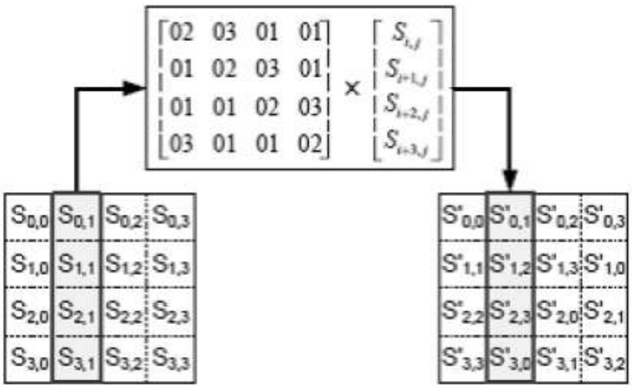

Fig.6 Mix Column Process

	BLOCKS IZE	OAES ENCRYPTION TIME	OAES DECRYPTION TIME	MAES ENCRYPTION TIME	MAES DECRYPTION TIME
0	0	0	0	0	0
1	200	0.07306695	0.144130468	0.078723431	0.150136471
2	400	0.144131184	0.288996458	0.157142639	0.298270941
3	600	0.212802649	0.426130772	0.232753038	0.444164991
4	800	0.286910772	0.569517136	0.309027433	0.594110966
5	1000	0.357120514	0.711867571	0.388439655	0.74558115
6	1200	0.431531429	0.85889554	0.464734077	0.886425018
7	1400	0.498572111	1.001305819	0.543958187	1.037644386
8	1600	0.571002483	1.146540165	0.618527889	1.181308985
9	1800	0.648367643	1.294424295	0.705809116	1.347166538
10	2000	0.718652487	1.439751625	0.777841568	1.482756615
11	2200	0.789165974	1.575108528	0.861928225	1.638389587
12	2400	0.859639406	1.725492477	0.941195965	1.798029661
13	2600	0.933243036	1.873767138	1.021160603	1.936397552
14	2800	1.013615608	2.016579628	1.237341166	2.339947224
15	3000	1.081787348	2.166396141	1.164149284	2.241556168
16	3200	1.148303032	2.296367645	1.248567104	2.383872271
17	3400	1.225673199	2.453509569	1.33632946	2.540692329
18	3600	1.304152012	2.593055487	1.421662569	2.693468332
19	3800	1.372518063	2.731688261	1.477969885	2.82988286
20	4000	1.444795132	2.901023626	1.560515404	3.043602705
	4200	1.502748251	2.991802454	1.656993151	3.155423403
22	4400	1.575759411	3.142236233	1.70720768	3.27212286
23	4600	1.660069942	3.379750729	1.78350544	3.409239531
24	4800	1.813122749	3.453919411	1.862156391	3.575967789
25	5000	1.787180901	3.587009668	1.936036348	3.712869167

Proposed architecture :

This research introduces an enhanced encryption algorithm designed to strengthen key security objectives—Integrity, Availability, and Confidentiality—during data transmission. The proposed method builds upon the symmetric key encryption framework, similar to the Advanced Encryption Standard (AES), by incorporating an additional step to enhance security [1].

Figure 8 depicts the structure of the modified AES algorithm. To assess its performance, multiple plaintext inputs were encrypted using both the conventional AES and the modified version (M-AES). The resulting ciphertexts were then examined and compared by quantitatively measuring the avalanche effect [3]. It was observed that the avalanche effect is influenced not only by the algorithm's complexity but also by the characteristics of the encryption key & plaintext [4].

Table 2 shows a comparison of the performance between the standard AES and the modified AES.. The results indicate that the inclusion of the additional Add Round Key step leads to a negligible increase in execution time. Specifically, for larger block sizes, the difference in execution time is approximately 0.13 seconds, demonstrating that the security enhancement does not substantially compromise efficiency [5][15]. Table 2. Performance Comparision

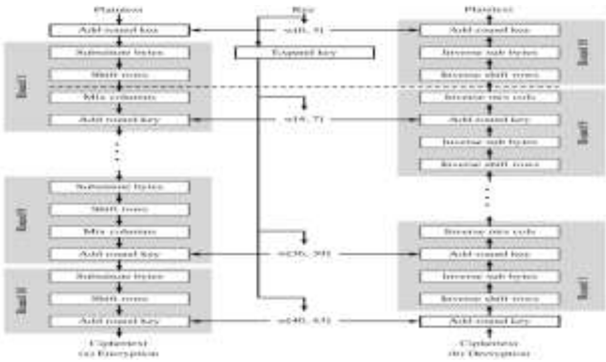

Fig.7 AES Encryption and Decryption

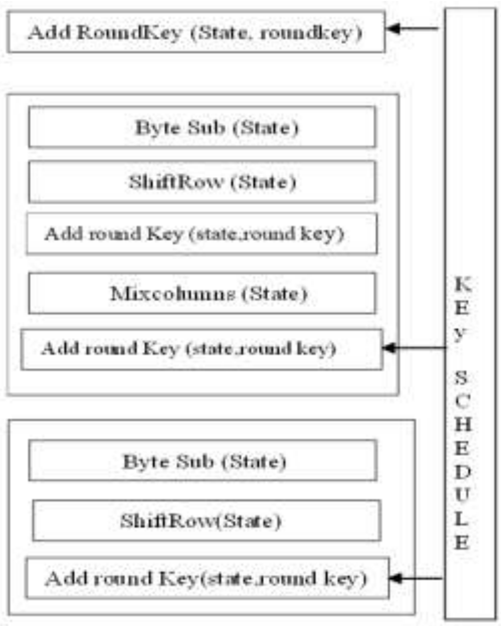

Fig. 8 Modify AES Architecture

Avalanche Effect and Testing : In cryptography, the avalanche effect is a key characteristic of encryption algorithms, where a minor alteration in the plaintext or encryption key results in a substantial and unpredictable change in the cipher text [6]**.** This property is essential for maintaining the robustness and security of cryptographic systems [16].Simply put, the avalanche effect measures

https://doi.org/10.46335/IJIES.2025.10.7.4 e-ISSN: 2456-3463
Vol. 10, No. 7, 2025, PP. 16-21
International Journal of Innovations in Engineering and Science, www.ijies.net

how significantly the cipher text changes when even a single bit of the plaintext or key is altered. Ideally, changing a single bit in the input should cause at least half of the bits in the ciphertext to be altered [7]. The results of these experiments are presented in Tables 3 and 4 [8][12][17].

Table 3 Avalanche effect for Key

	key	Cipher text	bits flipped	avalanche effect
0	A9B5ED7585C8B15D7454ED271AA3A3A3	AD512E36316802EFF789587EE2EFA6BB	0	0
1	29B5ED7585C8B15D7454ED271AA3A3A3	E44EC5EADB225DF51DF995859EAE6AF6	57	44.53125
2	69B5ED7585C8B15D7454ED271AA3A3A3	369FF04CF3D35BBD5683E29CA0F41F03	62	48.4375
3	49B5ED7585C8B15D7454ED271AA3A3A3	F1D646890A379C3E40C7F87854E78491	65	50.78125
4	59B5ED7585C8B15D7454ED271AA3A3A3	76488C9CB6C573005FBF6E69F19FF3BC	64	50
5	51B5ED7585C8B15D7454ED271AA3A3A3	00B3EF1EB598D856A10313D7669B2DD5	68	53.125
6	55B5ED7585C8B15D7454ED271AA3A3A3	2D4F16BDEEC5E7A899F00769823FD72E	62	48.4375
7	57B5ED7585C8B15D7454ED271AA3A3A3	C0CBFDD936870623E792569214006E82	59	46.09375
8	56B5ED7585C8B15D7454ED271AA3A3A3	BC1429B4F6C619F700F34BFAF9CDD177	69	53.90625
9	5635ED7585C8B15D7454ED271AA3A3A3	3D44B310A4D180D373DF314507BD4778	69	53.90625
10	5675ED7585C8B15D7454ED271AA3A3A3	36FEBFFBB1EBA11E9D6E63E1A012AB2A	60	46.875
11	5655ED7585C8B15D7454ED271AA3A3A3	7B29242647969BF572EE5468F37F2737	75	58.59375
12	5645ED7585C8B15D7454ED271AA3A3A3	FDB751DB2190666E8A1899B8C09FB278	70	54.6875
13	564DED7585C8B15D7454ED271AA3A3A3	700F5471A4DF1596D4A62BC144851849	50	39.0625
14	5649ED7585C8B15D7454ED271AA3A3A3	64A3BAE3560A192101653F9A6DDC6024	55	42.96875
15	564BED7585C8B15D7454ED271AA3A3A3	2D0FA8366FF47027E4B3C3BA2C10162C	67	52.34375
16	564AED7585C8B15D7454ED271AA3A3A3	D07C0EC51B5FFF8D404C7812F3A78713	69	53.90625
17	564A6D7585C8B15D7454ED271AA3A3A3	13D478C8DEC1C819894F291CF8EFA35F	61	47.65625
18	564A2D7585C8B15D7454ED271AA3A3A3	E761BC212DCE6AD5983ED2B4AE00A56E	66	51.5625
19	564A0D7585C8B15D7454ED271AA3A3A3	9BD668E0DB520F355033841EAA8A9D6B	64	50
20	564A1D7585C8B15D7454ED271AA3A3A3	3680A89B9F9AE8A0D52CF3BBD8532D9D	60	46.875

Table 4 Avalanche effect for plain Text

	plaintext	Cipher text	bits flipped	avalanche effect
0	B9B5ED7585C8B15D7454ED271AA3A3A3	AD512E36316802EFF789587EE2EFA6BB	0	0
1	39B5ED7585C8B15D7454ED271AA3A3A3	B7FFC781D85BB0AB7C26EB15B8D5F807	56	43.75
2	79B5ED7585C8B15D7454ED271AA3A3A3	B0876BCDCC9AA995DE1372C0F2E7F075	60	46.875
3	59B5ED7585C8B15D7454ED271AA3A3A3	B2AFCF4B18D21B7069D0BD76A4F5F63C	62	48.4375
4	49B5ED7585C8B15D7454ED271AA3A3A3	BF3ABBDFFDC5E305FA06DB61AF86615D	60	46.875
5	41B5ED7585C8B15D7454ED271AA3A3A3	116CA34D8D490529EB3898FD1DF7EB9C	64	50
6	45B5ED7585C8B15D7454ED271AA3A3A3	25BDF7FE322D24AA9B58F6A0D7826459	67	52.34375
7	47B5ED7585C8B15D7454ED271AA3A3A3	88453CA26E1C88E84724FB48F5E76D9F	74	57.8125
8	46B5ED7585C8B15D7454ED271AA3A3A3	E19D2F35CCDF12477ED52744CB513C08	65	50.78125
9	4635ED7585C8B15D7454ED271AA3A3A3	EDC5CB74833F572E14C80D8E2590A71F	70	54.6875
10	4675ED7585C8B15D7454ED271AA3A3A3	CF501F588D190F6A02467AB96936F0E6	64	50
11	4655ED7585C8B15D7454ED271AA3A3A3	C9238742F4DB3BD1D2D4F4C4952299DB	59	46.09375
12	4645ED7585C8B15D7454ED271AA3A3A3	51F4A47C39E06BE3B0390223EF3E6165	69	53.90625
13	464DED7585C8B15D7454ED271AA3A3A3	C707B1B3AECDB5F7E1350CBF243F0C47	62	48.4375
14	4649ED7585C8B15D7454ED271AA3A3A3	20C00205B590DC14919EC77AED94D330	60	46.875
15	464BED7585C8B15D7454ED271AA3A3A3	AE66E4479643D4AEB65A695656BB75A3	71	55.46875
16	464AED7585C8B15D7454ED271AA3A3A3	E8D211134AA68FE63D57EE9985D47789	58	45.3125
17	464A6D7585C8B15D7454ED271AA3A3A3	F1FC4759A2A892C7E46E404D1904375B	65	50.78125
18	464A2D7585C8B15D7454ED271AA3A3A3	03C510B1508B6A3398A0F641E81347ED	59	46.09375
19	464A0D7585C8B15D7454ED271AA3A3A3	E8A76BC950AC08EC1262141452E4A3CC	66	51.5625
20	464A1D7585C8B15D7454ED271AA3A3A3	7BD8FDFB54B9748156DBA37251C93FC7	60	46.875

III. Conclusion

The AES algorithm offers a robust level of security combined with efficient implementation, making it a reliable encryption standard for the foreseeable future [9]. The analysis in this paper demonstrates that even a small change, such as flipping a single bit in the plaintext or key, leads to a substantial change in the ciphertext [13]**.**

Performance evaluations indicate that the additional encryption step introduced does not significantly impact the overall processing time. The experimental results demonstrate an **avalanche effect** of approximately **52.34%** when altering a single bit in the plaintext and about **53.90%** when modifying one bit in the key. These outcomes confirm that the encryption process exhibits strong sensitivity to input changes, ensuring that the ciphertext is substantially different with each minor variation, thereby enhancing overall security [10][14][18].

IV. References

[1] *Rohit Verma, Aman Kumar Sharma, "Cryptography: Avalanche effect of AES and RSA", International Journal of Scientific and Research Publications, Volume 10, Issue 4, April 2020.*

[2] *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*

[3] *Amish Kumar , Mrs. Namita Tiwari, "EffectiveImplementation andAvalanche Effect Of AES", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 3/4, August 2012.*

[4] *Ajeet Singh, "A New Approach to Enhance AvalancheEffect in Aes to ImproveComputer Security" , Journal ofInformation Technology & Software Engineering, ISSN:2165-7866, Volume 5 • Issue 1 • 1000143.*

[5] *Md. Enamul Haque, SM Zobaed, Muhammad Usama Islamy, and Faaiza Mohammad Areef, "PerformanceAnalysis of Cryptographic Algorithmsfor Selecting Better Utilization on ResourceConstraint Devices", https://www.researchgate.net/publication/330879356.*

[6] *T. Jamil, "The rijndael algorithm," IEEE potentials, vol. 23, no. 2, pp. 36–38, 2004.*

[7] *A. Sachdev and M. Bhansali, "Enhancing cloud computing security using aes algorithm," International Journal of Computer Applications, vol. 67, no. 9, 2013.*

[8] *I. M. A. Fadul and T. M. H. Ahmed, "Enhanced security of rijndael algorithm using two secret keys," International Journal of Security and its applications, vol. 7, no. 4, pp. 127–134, 2013.*

[9] *S. Zobaed, M. A. Salehi, A. Zomaya, and S. Sakr, "Big data in the cloud." 2019.*

[10] *K. Akhil, M. P. Kumar, and B. Pushpa, "Enhanced cloud data security using aes algorithm," in 2017 International Conference on Intelligent Computing and Control (I2C2). IEEE, 2017, pp. 1–5.*

[11] *M. S. A. Forhad, S. Riaz, M. S. Hossain, and M. Das, "An improvement of advanced encryption standard," International Journal Of Computer Science And Network Security, vol. 18, no. 11, pp. 159–166, 2018.*

[12] *R. Mehla and H. Kaur, "Different reviews and variants of advance encryption standard," International Journal of Science and Research (IJSR), ISSN (Online), pp. 2319–7064, 2014.*

[13] *P. Pimpale, R. Rayarikar, and S. Upadhyay, "Modifications to aes algorithm for complex encryption," IJCSNS International Journal of Computer Science and Network Security, vol. 11, no. 10, p. 183, 2011.*

[14] *R. Arora, A. Parashar, and C. C. I. Transforming, "Secure user data in cloud computing using encryption algorithms," International journal of engineering research and applications, vol. 3, no. 4, pp. 1922–1926, 2013.*

[15] *G. N. Selimis, A. P. Fournaris, and O. Koufopavlou, "Applying low power techniques in aes mixcolumn/invmixcolumn transformations," in 2006 13th IEEE International Conference on Electronics, Circuits and Systems. IEEE, 2006, pp. 1089–1092.*

[16] *P. Kumar and S. B. Rana, "Development of modified aes algorithm for data security," Optik, vol. 127, no. 4, pp. 2341–2345, 2016.*

[17] *P. Deshmukh and V. Kolhe, "Modified aes based algorithm for mpeg video encryption," in International Conference on Information Communication and Embedded Systems (ICICES2014). IEEE, 2014, pp. 1–5.*

[18] *Y. Khatri, R. Chhabra, N. Gupta, A. Khanna, and D. Gupta, "Secure modified aes algorithm for static and mobile networks," in International Conference on Innovative Computing and Communications. Springer, 2020, pp. 389–399.*

[19] *F. M. Amine and G. Abdelkader, "Hybrid approach of modified aes," in Cryptography: Breakthroughs in Research and Practice. IGI Global, 2020, pp. 129–141.*

[20] *M. E. Haque, S. Zobaed, M. U. Islam, and F. M. Areef, "Performance analysis of cryptographic algorithms for selecting better utilization on resource constraint devices," in 2018 21st International Conference of Computer and Information Technology (ICCIT). IEEE, 2018, pp. 1–6.*