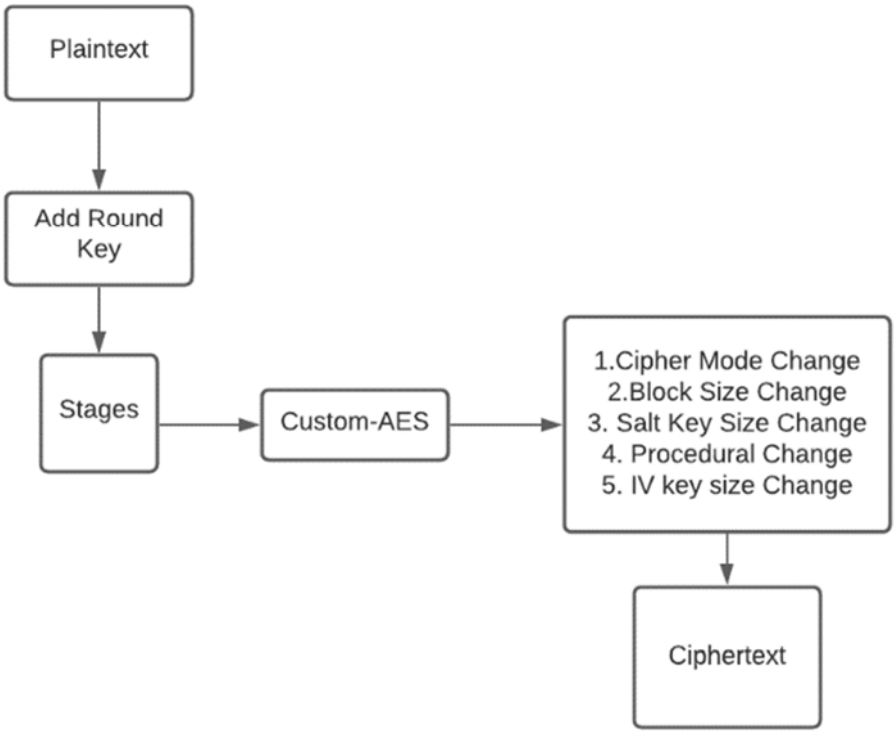

Fig.1. Block Diagram of the Proposed Custom-AES

3.1 *Model development*

The development model flow is the following:

- For the improved AES algorithm, 128-bit key length is used.
- Encryption and decryption of the proposed method are identical to standard AES algorithms.
- With the conventional AES algorithm the round process feature is identical.
- Another process of modification is undertaken in cipher mode, block size, salt key size, IV key sizes and procedural modifications.
- As a device input, we will take 256-bit data.
- These outputs then form an encrypted data block of 256 bits.

4. Results and Discussion

The changes to the AES were assessed in terms of the avalanche effect. The Avalanche effect is a useful feature of the block ciphers, which ensures that output text for a single bit is changed at least 50 percent. The execution time is the time it takes for the algorithm to encrypt or decrypt a certain input document.

4.1 *Avalanche Effect*

It is necessary to see whether the avalanche effect occurs or not to decide the security of an algorithm. Avalanche effect is an algorithm that diffuses and confuses more than 50%. The Avalanche effect is Where changing the plaintext or the key just one bit while maintaining the other constantly. It changes at least 50% of the ciphertext.. F1{i,j}n here {i,j}n meet avalanche requirements, if at least half a bit of the input bit changes to the output bit. Where I and j are bits of input and output, according to avalanche standards

$$\frac{1}{2^n}\sum_{j=1}^{n} W\left(a_j^n\right) - \frac{n}{2} \quad (1)$$

Where
$W\left(a_j^n\right) = \sum_{j=1}^{n} a_j^n$ x: {0,1}

Total change in j^{th}avalanche variable computed over whole input size 2^nin the range $0 \leq W(a_j^n) \leq 2^n$ From equation (1) we can manipulate avalanche parameter of i as

$$K_{avalanche}(i) = \frac{1}{n2^n}\sum_{j=1}^{n} W(a_j^n) - \frac{1}{2}$$

With the above formula, we proved that the probability of change of output bit when only one or bit of input is changed is half.
Also, can be defined by

$$avalanche\ Effect = \frac{number\ \ of\ bits\ flipped\ in\ cipher\ text}{number\ \ of\ bits\ in\ cipher\ text}$$

One of the main features of cryptography is the Strict Avalanche Criterion (SAC). According to the SAC, changes in 1-bit plain text affect more than half of the bits. Or, switching to a 1-bit key can affect the cipher-text more than half of the bits. The Avalanche Effect is named.
However, changing one bit of the plaintext or one bit of the key in several pieces of the cipher text can generate a shift. The Avalanche effect is called this property. The above equation can be used to measure the Avalanche Effect. Due to the one- bit fluctuation in plaintext, which keeps the encryption key constant, the output of the proposed algorithm is evaluated by means of Avalanche effect.

5. Measuring the Avalanche Effect

5.1. *Case i: Changing One character in a Word-keeping Key Constant*

The Custom-AES effect obtained a higher avalanche effect than the traditional AES algorithm based on calculated results in Table 1. The traditional AES had an avalanche of 37.03% while the Custom-AES had an avalanche of 62.9%. The number of bits flipped for Custom-AES is 17 and for conventional AES is 10.

Algorithm	Cipher1 (Encrypta)	Cipher 2(Encryptb)	Number of bits flipped	Avalanche Effect in %
Custom AES	NUNDNCI668E1DBNUEKIJSD46E UHIS	NUNDNCI668JISDYHIJNA5FFFW EF5	17	62.9
AES	SSMIBD28FKISF85USR86YNIOS6 H328	SSMIBD28FKISF85USHATSRR622 E5A	10	37.03

Table-1. Avalanche effect comparison on Custom- AES and AES by changing one character in a word keeping key constant

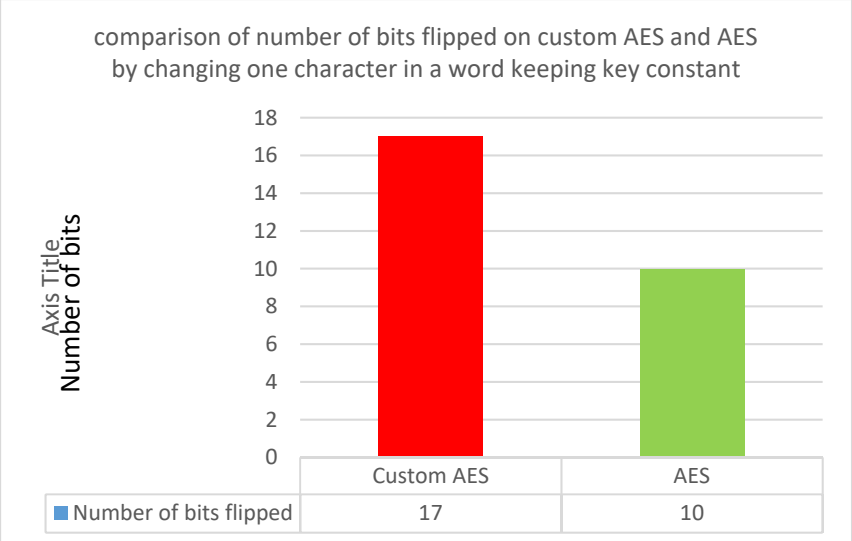

Fig. 2. Comparison of number of bits flipped on custom AES and AES by modifying one character in one word holding the key constant

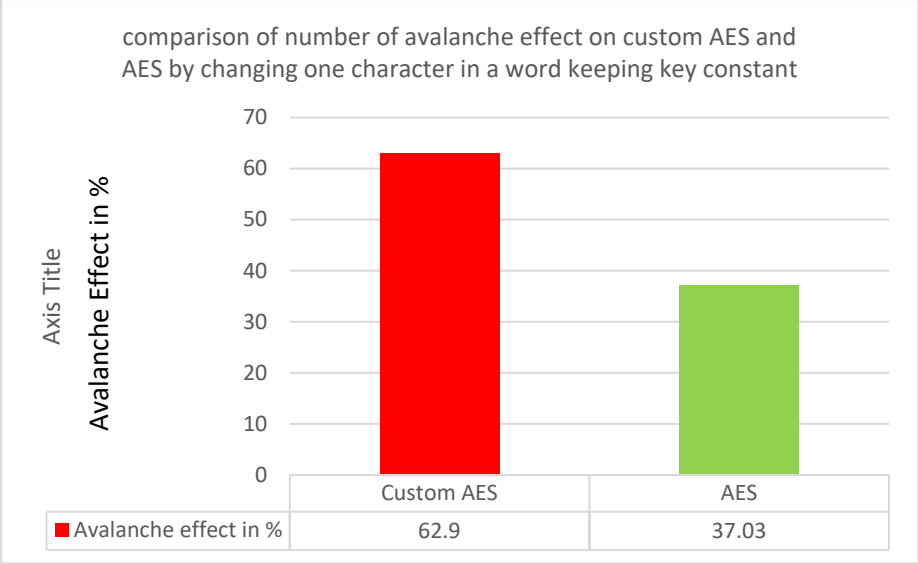

Fig. 3. Comparison of number of avalanche effect on custom AES and AES by modifying one character in a word holding the key constant

5.2. Case ii: Changing one number in a set of numbers keeping key constant

The avalanche effect achieved after changing one number in a number set is shown in Table 2. Table 2. As a result, the avalanche effect achieved by Custom-AES by 58.33% compared with the traditional AES algorithm by 33.33%. The number of bits flipped for Custom-AES is 14 and for conventional AES is 8.

Algorithm	Cipher1 (012345)	Cipher 2(012347)	Number of bits flipped	Avalanche effect in %
Custom AES	FV595SDV2DF85SD65V1V8S6D	FV595SDV2YG58DF59S5S98SD	14	58.33
AES	HYSJOD68V1SAU12G58A93A5F	HYSJOD68V1SAU12G84D8569F	8	33.33

Table 2. Avalanche effect comparison on Custom- AES and AES by changing one number in a set of numbers keeping key constant

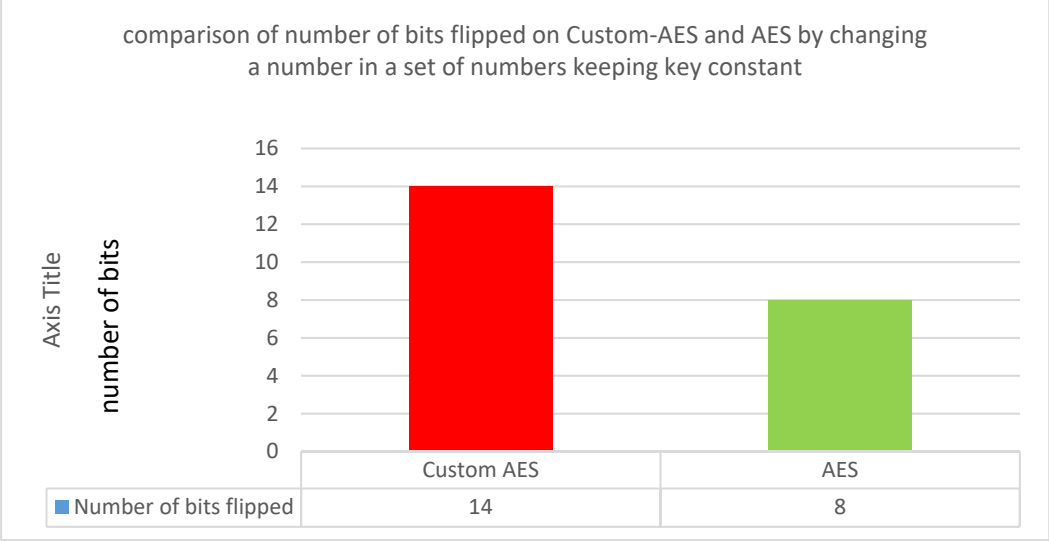

Fig. 4. Comparison of number of bits flipped on Custom-AES and AES by changing a number in a set of numbers keeping key constant

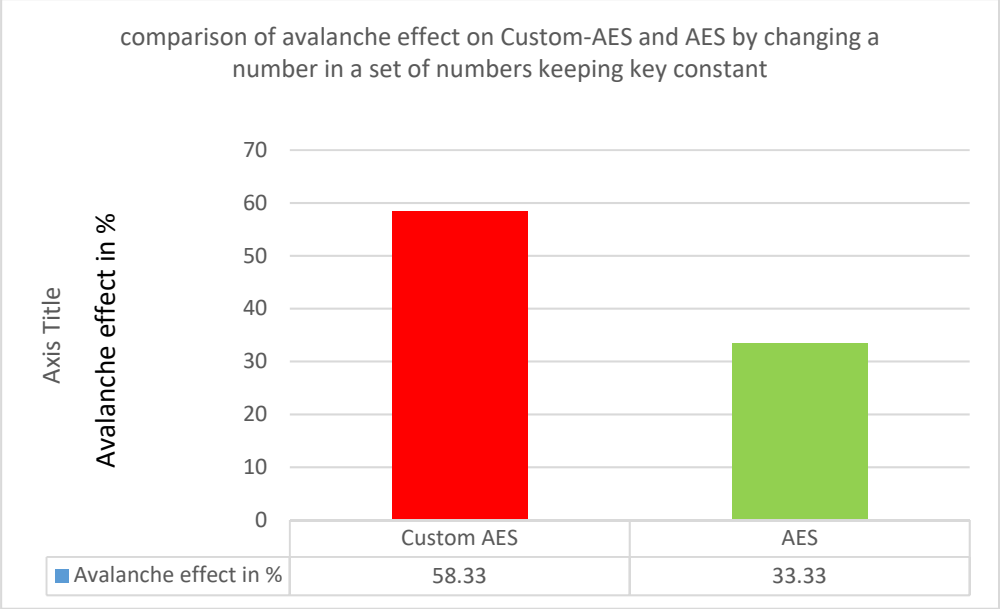

Fig.5. Comparison of the Avalanche effect on Custom-AES and AES by changing a number in a set of numbers keeping key constant

5.3. Case iii: Changing one character in a sentence keeping key constant

The conventional AES, as shown in Table 5, has an avalanche effect of 42.14%, whereas Custom-AES has an effect of 57.6%. It demonstrated a greater avalanche effect was achieved by Custom-AES. The number of bits flipped for Custom-AES is 715 and for conventional AES is 523.

Algorithm	Cipher1(Tamilnadu is my state) Total bits	Cipher2(Tamilnadu in my state) Total bits	Number of bits flipped	Avalanche effect in %
Custom AES	1241	1241	715	57.6
AES	1241	1241	523	42.14

Table3. Avalanche effect comparison on Custom-AES and AES by changing one character in a sentence keeping key constant

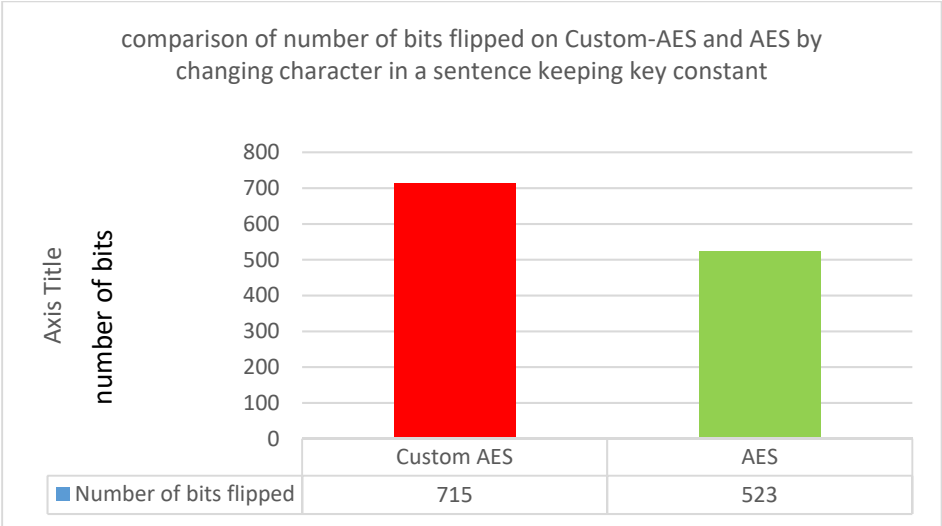

Fig.6. Comparison of number of bits flipped on Custom-AES and AES by changing character in a sentence keeping key Constant

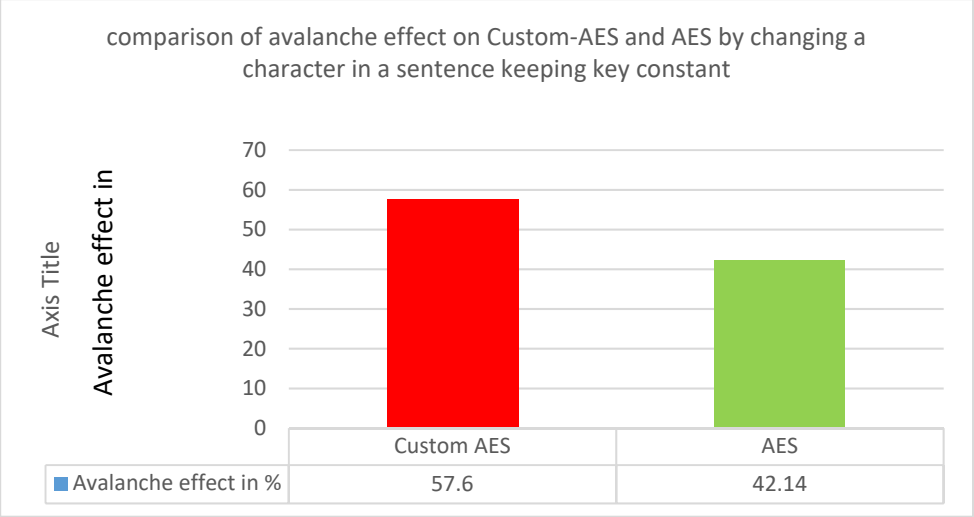

Fig. 7. Comparison of the avalanche effect on Custom-AES and AES by changing a character in a sentence keeping key constant

6. Conclusion

The method is being proposed for enhancing the traditional AES algorithm by modifying cipher mode, block size, salt key, IV key size and procedural modifications. The Custom-AES algorithm is judged by the avalanche effect and the results show the higher avalanche effect of the Custom-AES. The Avalanche Effect of the proposed method is effective and powerful from the experimental results. It supports the 256-bit block, which contributes to increased diffusion and uncertainty. The algorithm is stable. The heavy impact of avalanche. The high level of avalanche effect was reported because the traditional AES could still be improved and it is advisable to use the avalanche effect as a performance assessment method for more researchers. The proposed device is therefore good and not crackable and resistant to brute-force attacks.

Reference

[1] P.Karthigaikumar, Soumiya Rasheed"Simulation of Image Encryption using AES Algorithm" IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011
[2] Diaa Salama Abd Elminaam, Hatem Mohamad Abdual Kader,Mohiy Mohamed Hadhoud, "Evalution the Performance of Symmetric Encryption Algorithms", international journal of network security vol.10,No.3,pp,216-222,May 2010.
[3] Nidhi Singhal, 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.
[4] Prof.Gajendra Singh, Preeti Shukla, "Design and Development of New symmetric Cryptography Protocol to Improve Text Security" published by International Journal of Advanced Research inComputer Science and Software Engineering, Volume 4, Issue 11, November 2014, ISSN: 2277 128X.
[5] Debajit Sensarma, Samar Sen Sarma, "GMDES: A GRAPH BASED MODIFIED DATA ENCRYPTION STANDARD ALGORITHM WITH ENHANCED SECURITY" published by IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308, Volume: 03 Issue: 03 | Mar-2014.
[6] Sriram Ramanujam and Marimuthu Karuppiah, "Designing an algorithm with high Avalanche Effect" published by IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.1, January 2011.
[7] Rajdeep Chakraborty, Sonam Agarwal, Sridipta Misra, Vineet Khemka, Sunit Kr Agarwal, J. K. Mandal, "Triple SV: A Bit Level Symmetric Block Cipher Having High Avalanche Effect" published by (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 7, 2011.
[8] http://en.wikipedia.org/w/index.php?title= Confusion_and_diffusion&oldid=389143741
[9] http://en.wikipedia.org/w/index.php?title= Avalanche_effect&oldid=422317482
[10] Manisha S. Mahindrakar, "Evaluation of Blowfish Algorithm based on Avalanche Effect" published by International Journal of Innovations in Engineering and Technology (IJIET) Vol. 4 Issue 1 June 2014, ISSN: 2319-1058.
[11] Akash Kumar Mandal, Mrs. Archana Tiwari, "Analysis of Avalanche Effect in Plaintext of DES using Binary Codes" published by International Journal of Emerging Trends and Technology in Computer Science (IJETTCS) Volume 1, Issue 3, September-October 2012.
[12] Yushu Zhang, Di Xiao, "An image encryption scheme based on rotation matrix bit-level permutation and block diffusion" in Commun Nonlinear Sci Numer Simulat-Sciencedirect 19 (2014) 74-82.