Improvement in the Performance and Security of Advanced Encryption Standard Using AES Algorithm and Comparison with Blowfish

Amit Verma [1*], Simarpreet Kaur [1], Bharti Chhabra [3]

[1]M. Tech. Research Scholar, Computer Science & Engineering, Chandigarh Engineering College

[3]Assistant Professor, Computer Science& Engineering, Chandigarh Engineering College, Landran, Punjab, India

[1*] Professor and Head of Department, Computer Science& Engineering, Chandigarh Engineering College, Landran,Punjab, IndiaDramitverma.cu@gmail.com

Abstract-Background\Objective: - The origin of cryptography is found in Roman and Egyptian culture. Cryptography is thousand years old process to encrypt the messages. In its ancient form, people use cryptography to hide their messages that they want to keep secret from other by substituting the part of the message with symbols, numbers or pictures. With the increase in technology the need of cryptography is also increased which gives rise to new cryptographic algorithms such as DES, 3DES, AES and Blowfish.

Statistical Analysis: - AES is a symmetric key encryption algorithm.AES is made more secure and reliable then the existing one.AES is combined with segmentation and validation algorithm to improve the performance of the AES. Key expansion is done to make the AES more secure. The processes are pipelined to increase the speed of AES.

Findings: - AES is made more secure and the performance of the AES is also improved in order to increase the reliability.

Improvements/Applications: - With proposed AES, the speed to encrypt the data is increased within less time. Whereas, existing AES takes more time to encrypt with low speed. In this, the 128 bits block ciphers are pipelined in order to increase the performance of the AES. Also the security of the AES is improved by making enhancement in the key matrix of the applied key expansion. AES can be used for secure communication such as in image encryption, ATM networks and secure storage such as confidential documents, government documents and personal storage devices.

Keywords: - Galois Field, S-Box, Segmentation and Validation, XOR, Sub-bytes.

Introduction : From many generations, the fundamental need of human beings is :-(i) to communicate and share information and (ii) Communicate securely. These two needs gave origin to the art of coding messages which is known as cryptography. It is the process of converting the secret messages, information or data into an unreadable form in order to protect it from an unauthorized person, according to some rules. Although, cryptography has been used for thousands of years, it is an adolescent science. It is an ancient way used to encrypt the messages.[1] Encryption is the process in which the plaintext is converted into a ciphertext, this conversion of text is based on algorithms. Encryption can be performed in many ways such as replacing the message with numbers, symbols and pictures. In ancient times, people also use different types of voices to deliver their messages securely to the receiver. The word "cryptography" is extracted from the two Greek words "krypto" which means secret or hidden and "graphein" which means writing.[2] Cryptography is observed with the advent of writing. The advancement of human beings to got settled in tribes and kingdoms purposed ideas such as battles and politics. These ideas promote the perquisite to converse confidentially with specific recipients which results in the continuous expansion of cryptography.[3] It is the oldest field of study and its origin can be observed in Egyptian and roman civilizations. Following is the comprehensive history of cryptology:-

About 4000 years ago, Egyptians used to communicate secretly with each other by sending their messages written in "hieroglyph". This technique can be called as the first evidence of cryptography. These codes were secret which are only known to the writers who convey messages in place of kings.[4]

About 1500 BC, Assyrian merchants started using "intaglio" which was a type of cryptography. They use intaglio to disappear the fear of misrepresentation in market. They establish a primitive form of recognition. Intaglio was a flat stone with impressions on it, which was distinctive to a particular trader. In this way, people could be insured of whom they were literally marketing within business agreements. By applying this procedure they were developing "digital signatures”. Everyone knew that a specific signature belongs to a specific merchant and only he had an intaglio to create that signature.

During 500 to 600BC, scholars move on to employ easy mono alphabetic substitution ciphers which is well known as ATBASH. The atbash cipher is a Hebrew code, which performs by swapping the first alphabet of the message by the last alphabet, second alphabet of the message by second last alphabet and so on. This swapping of alphabets is done according to some confidential rule. This rule became a key to fetch the original message back from the jumbled message. ATBASH was one of a few Hebrew ciphers of the era.[5]

In 487 BC, The Greeks used a tool known as "scytale" which was applied to conduct a transposition cipher. A scytale was consisted of a cylinder around which thin, long leather was wrapped on which the message was written. This leather was taken off and was worn as a belt. The former Greeks used this cipher to converse during military campaigns. The receiver uses a rod of the exact diameter on which the leather was wrapped to read the encrypted message. It was a fast and error free technique to deliver messages secretly. The main disadvantage of this technique was that it can be easily broken.

In 100-44 BC, Julius Caesar employed an easy substitution with ordinary alphabets by just moving the letters to a fixed amount. This method was less powerful than ATBASH, but gained popularity. In this, shift by 3 rules was applied for example A was replaced by D, B was replaced by E and so on.[6]

In 725-790 AD, an Arabian wrote book on cryptography by getting inspiration from result of a cryptogram in Greek for the Byzantine ruler. The result depends on the known plaintext at the beginning of the message which was an excellent cryptanalytic process, worked in World War II against Enigma process.

In 1466, Leon Battista Alberti formulated and produces the initial polyalphabetic cipher by inventing a cipher disk to clarify the process. This sort of cipher was evidently not failed till the 1800's. Alberti too wrote completely on the state of technique in ciphers, except his own creation. Alberti also used his disk for enciphered code. This method was much vigorous as compared to the terminology used by the experts of that era.[7]

In 1518 Johannes Trithemius wrote the introductory printed book on cryptology. In this a stenographic cipher was developed in which each letter was shown as a word taken from a concatenation of columns. The concluded series of words would be a authorized prayer. In this Polyalphabetic cipher was explained and the code of converting alphabets with each letter was also introduced.

In 1553 Giovan Batista Belaso introduced the code of utilizing passphrase as a key for iterated poly-alphabetic cipher. Then in 1563 Giovanni Battista Porta, establish a Diagraphic cipher by writing a text on ciphers. This categorizes ciphers as transposition, substitution and symbol substitution. The use of synonyms and spelling mistakes to confuse cryptanalyst is proposed. In poly-alphabetic representation the notation of a mixed alphabet is clearly introduced.[8]

In 1585, Blaise De Vigenere wrote book on ciphers, containing the initial authentic plaintext and ciphertext auto key procedure. In 1623 Sir Francis Bacon represent a cipher which now convey his name "a biliteral cipher" which is presently known as 5 bit binary encoding. Sir Francis proposed it as a stenographic device by applying alterations in type face to transfer each bit of the encoding.

In 1790, Thomas Jefferson, perhaps promoted by Dr. Robert Patterson, introduces his wheel cipher, which was re-invented in various types later and applied in World War II by the US Navy.

However cryptography was used throughout World War I, but the most prominent machine ever innovated was the Germans "Enigma Machine", which was used in World War II invented by Arthur Scherbius. This powerful and victorious electromagnetic device become the slave of the Germans in World War II and was consisted of three rotors. There is a plug board in Enigma that allows the user to exchange any letter for another letter at a mismatched place of the rotors. These plug boards help in increasing the number of collaborations of enigma settings by a factor of ten to fifteen. This benefit of enigma gave the German forces the confidence to use various types of enigmas for security reasons. The perfectly implemented operating methods made the Enigma unbreakable. But the polish mathematician, Marian Rajewski had failed the enigma machine.[9]

Earlier cryptography was used by government organizations and military only. But with the passage of time everything is changed. With the increase in technology cryptography is needed by everyone and everywhere to protect their information from an unauthorized attack. The modern encryption methods are not much different from ancient ones. Modern cryptography can be divided into two types: Symmetric cryptography and asymmetric cryptography. In symmetric Cryptography same key is used to encrypt or decrypt the messages and in asymmetric cryptography different keys are used to encrypt and decrypt the messages. Some important modern encryption systems that we use now are DES, Triple DES, RSA, Blowfish, Twofish and AES.[10]

Data Encryption System (DES) was a symmetric encryption algorithm. The national security agency in the interest of U.S. government working with Fiestel networks initiate DES, which is a block cipher used for protecting secret documents from unauthorized persons. In DES,64-bits key was used to encrypt or decrypt the data and it takes 64-bits block plaintext as an input, repeat algorithm 16 times and produces an output of 64 bit block cipher. This encryption algorithm was no longer successful and replaced by triple DES.

The triple DES also called 3DES is a symmetric key algorithm that was depicted to replace DES, which was used in industries mostly for financial organizations. In triple DES three 64 bit keys for complete key length of 192 bits. The technique was same as of DES but in 3DES three different keys was used. Triple DES is more reliable than DES; however it is much slower than the single DES.

RSA is an algorithm which is used in modern computers to encrypt and decrypt the data. It is asymmetric cryptographic algorithm in which two different keys are used, one key is kept public that means it can be given to everyone and other key is kept private. The outcome of RSA algorithm is enormous cluster of jumbo that takes attackers an absolute time and processing capacity to crack the code.[11]

Blowfish developed by Bruce Schenier, in 1993 is an additional algorithm created to replace DES. It is a symmetric block cipher that takes 64-bits block as an input and encrypts them separately. The variable key length of this algorithm is from 32 bits to 448 bits. It is a fast, compact, simple and secure algorithm. It is openly available in the public domain. Blowfish can be initiated in many e-commerce applications for protecting payments to password management mechanisms. It is the most flexible and fastest algorithm.[12]

Two fish is another algorithm designed by Bruce Schenier, in 1998.It is a symmetric block cipher that accept block sizes of 128 bits as an input and key sizes 128,192 or 256 bits. Twofish can be used perfectly in both hardware and software environments. Similar to blowfish, twofish is also freely available and fastest algorithm. Twofish can be used in encryption schemes such as GPG, PhotoEncrypt and TrueCrypt.[13]

AES stands for advanced encryption standard is a normalized form of Rijndael algorithm developed by two Belgian Cryptographers, Vincent Rijmen and Joan Daemen. It is six times faster than triple DES.AES accepts block sizes of 128,168,192,224 and 256 bits whereas key lengths of 128,192 and 256 bits. Advanced Encryption standard was adopted by the U.S. Government to safeguard its confidential information and is implemented on software and hardware to encrypt the sensitive data. It is a symmetric key encryption algorithm which means that same key will be used to encrypt and decrypt the meassages.AES is based on the concept of substitution and permutation. In contrast to DES,AES do not use Fiestel Network(Symmetric structure used in construction of block ciphers).AES works on 4x4 matrix of bytes and depending on the key size used to encrypt AES block cipher rounds will be performed to transform plaintext into a ciphertext. Plaintext is the text which we have before encryption and ciphertext is the text which we get after encryption.10 rounds will be performed for 128 bits key, 12 rounds for 192 bits key and 14 rounds for 256 bits key. In this algorithm XOR operations, octet substitution, row and column rotation and mix column are used. The main reason behind the success of the AES algorithm is that it is more secure, reliable, and easy to implement and could employed in adequate amount of time.[14]

1.1 Algorithm of AES

All the computations in AES are executed on bytes instead of bits. Therefore, 128 bits of plaintext is treated as 16 bytes. These 16 bytes are positioned in a matrix of four rows and four columns. In AES 10 rounds are performed for 128bit keys, 12 rounds for 192 bit keys, and 14 rounds for 256 bit keys. All of these rounds apply a different 128 bit key, deliberated from the original AES key.[15] Following is the Algorithm to encrypt the data:-

- **Step 1**:- Input a plaintext of 128 bits of block cipher which will be negotiated as 16 bytes.
- **Step 2**: - Add Round Key: - each byte is integrated with a block of the round key using bitwise XOR.
- **Step 3**:- Byte Substitution: - the 16 input bytes are substituted by examining S- box. The result will be a 4x4 matrix.
- **Step 4**:- Shiftrow: - Every row of 4x4 matrixes will be shifted to left. Entry which will be left placed on the right side of row.
- **Step 5**:- Mix Columns: - Every column of four bytes will be altered by applying a distinctive mathematical function (Galois Field).
- **Step 6**:- Add Round Key: - The 16 bytes of matrix will be contemplated as 128 bits and will be XORed to 128 bits of the round key.
- **Step 7**:- This 128 bits will be taken as 16 bytes and similar rounds will be performed.
- **Step 8**:- At the 10th round which will be last round a ciphered text will be produced.

Initially, the plaintext of 128 bits of block cipher will be input, which will be treated as 16 bytes. Then, each byte will be integrated with a block of the round key using bitwise XOR. From S-Box the 16 input bytes will be exchanged resulting 4x4 matrixes. Every row of this matrix will be shifted to left. Shifting will be done as follows:-

1) First row will be not shifted.
2) Second row will be shifted one position left.
3) Third row will be shifted two positions to the left.
4) Fourth row will be shifted three positions to the left[16]

As a result new matrixes will be produced containing same 16 bytes but shifted with respect to each other. In MixColumn, every column of the matrix will be transformed by applying mathematical function such as Galois Field. The 16 bytes of matrix will be considered as 128 bits and will be XORed to 128 bits of round key.[17]

1. Related Work

Many researches had done in the area of cryptography. With the advent of technology everything is done over internet which results in the up gradation of algorithms used to encrypt data .Advanced Encryption Standard (AES) is the most commonly used algorithm to encrypt messages or information. Researches done by many authors in order to improve the AES level of security and performance is represented here:-

In 18 author, Xing-Yuan Wang has suggested a novel image encryption algorithm. The cycle proceeds in bits of pixels and muddled system are employed for the encryption of the presented scheme. For cycle shift operations, arbitrary integers with the homogeneous size of the original image are created to scramble the plaintext image. Moreover, the muddled image impacts the introductory values of the chaotic system for the additional encryption process, which magnify the susceptibility of plaintext images of the system. The muddled image is encrypted into the ciphered image through the keys, which are assembled by the chaotic system. The simultaneous experiments and theoretical examination specifies that the proposed strategy is praiseworthy and accomplished to resist comprehensive and statistical attack.

In 19 author, ChristofPaar, composed an article on all preferable applied cryptography and data security. In this paper all recommended encryption algorithms and their structure along with their advantages and disadvantages have discussed in detail.

In 20 author, Creighton Hager, discusses the performance on comparative analysis of various encryption algorithms on various forms of data. This research has expressed that blowfish outperforms all other encryption algorithms. Blowfish is the best, unbreakable and rapid encryption algorithm than others.

In 21 author, Gary Kessler, analyze an abstract of cryptography. This paper has proposed the ample source for the cryptography algorithms. The four main principles of cryptography such as authentication, Confidentiality, Integrity, and Non-repudiation were analyzed. In secret key cryptography, an individual key is employed for both encryptions and decryption. Public-key cryptography is the most successful development in the area of cryptography in the last 300-400 years, which use non-identical keys for encryption and decryption process.

In 22 author , Alaa Yasen Taqa and Aos Alaa Zaidan introduces a combined approach among steganography and cryptography. This approach will emerge high rate and high secure data which is concealed using secret key steganography and AES Rijndael method. Also, in this paper the use of approaches for concealing data and its organization is examined. Moreover they have also made the AES algorithm more robust.

In 23 author, Mohammadi proposed the substantial approaches for protection and also discussed a new solution, which significantly expands the protection of Internet polls and the precision of their results. The proposed solution has two stages: first is the establishment stage in which the poll content and CAPTCHA test are oriented and the second stage is the utilization stage, at this stage vote computing work is done. The CAPTCHA that is utilized in the suggested approach is an image-based CAPTCHA. For the level of choosing, an Internet user has to haul his or her suitable poll alternative demonstrated in the manner of portable text object and drop it on to the image of an object specified by the CAPTCHA. The presented system is feasible, vigorous, and resistant. One of the supremacy of the process is that it can be used by all generations.

In 24 author, Pitchaiah, Philemon and Praveen presented a 128 bit AES encryption and decryption using Advanced Encryption Standard (AES).It is collaborated using Virology code which can be simply executed on to FPGA. The algorithm consists of three main parts cipher, inverse cipher and Key Expansion. Cipher transforms data to meaningless form known as ciphertext. Key expansion creates a key schedule that is used in cipher and inverse cipher process. Cipher and inverse cipher consists of special number of rounds. For the AES algorithm, the number of rounds to be accomplished during the implementation of the algorithm uses a round function that is composed of four different transformations: Sub-Bytes, Shift Row, Mix columns and round key.

In 25 author, Navita Agarwal presented a research, where they employed compression, encryption and steganography on the digital image data. In this paper, pixel rearranging dependent symmetric encryption algorithm such as DCT for compression, WinRAR to Image steganography are used to achieve the proposed model.

In 26 author, Milind Mathur describes a study on the encryption algorithms. This comprehensive study on encryption algorithms describes all of the favorable and important algorithms. This study also states that blowfish is the best encryption algorithm and dominate all others. Blowfish takes minimum time and yield maximum throughput.

In 27 author, Sasan Adibi describes voice authentication capability. The voice attributes of a deliberated person requiring taking part in a communication channel will be categorized and organized. This requires a low overhead voice authentication proposal, which features standardization and scaling of the voice frequency harmonics. The potential of this system is examined using visual development environment, following a complete security analysis.

In 28 author, Abdouli put forward an algorithm related to the security of various cryptosystems based on distinct computational stable issues. Many prevalent cryptographic strategies are based on the many theoretical complications such as factoring and discrete logarithms. These firm issues are assumed to be inadaptable for classical algorithms. It is required to evaluate new classes of another candidate of vigorous difficulties that have aggressive difficulties to both average and quantum computers, for example, error improving codes, matrix problems, scrambled groups and subset product. In this paper, focus is done on the regulating hard problems and their applications to cryptography.

In 29 author, Verma O.P. depict two main features that recognize and distinguish one encryption algorithm from another and its potential to safeguard the secured data opposed to attacks, its speed and capability in doing so. This paper exempts a performance differentiation between four of the most popular encryption algorithms: DES, 3DES, Blowfish and AES (Rijndael). The contrast has been supervised by conducting many encryption settings to practice different sizes of data blocks to evaluate the algorithm's encryption/decryption speed.

2. Proposed AES Algorithm

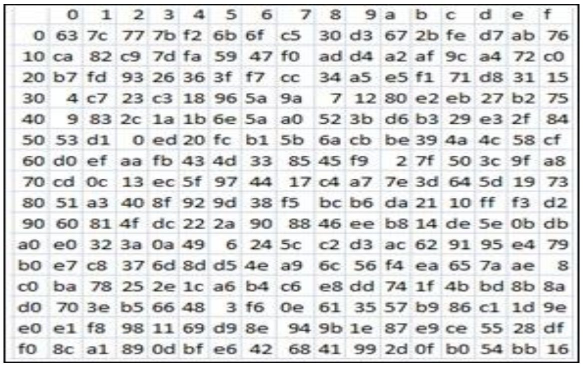
AES is the predominantly used encryption algorithm for encrypting and decrypting data. However, in existing AES there are some drawbacks such as lower throughput and takes more time to encrypt data. It also has some security issues. All these problems are resolved in the proposed AES. The proposed AES has been depicted with three substantial stages of progression. The initial phase of development includes execution of improved AES for altered window size or block size. In the second phase for expansion improvements are done in the key matrix. In the third phase the size and the shape of the S-box is improved to make AES more powerful and competent. In the last phase data validation and segmentation algorithm is developed to make the AES suitable for wider number of cases. Following is the detailed discussions of the three main phases used in the development of the proposed AES:-

Phase 1:-Programming Optimization

In order to attain rapid implementation of AES algorithm for software systems an improved version of AES encryption is designed. In the proposed AES to make the entire system run in a faster speed, several methods have been used in the data pass processing. Firstly, the input digits have been increased to 128 bits. This will enhance the operating speed of the system. These 128 bits are situated at the input terminal. Simultaneously all data will enter into the encryption and decryption system. This will decrease the data entering and passing time significantly.[30] Following is the algorithm for the construction of the S-box:-

- **Step 1**:- Provide the multiplicative inverse of the input number in two 8-bit unidentified variables supposed to be 'y' and 'z'.
- **Step 2:-** Change the value 'y' one bit towards left, if 'y' has high bit of one, form the lower bit of 'y' one, else the low bit of 's' is zero.
- **Step 3**:- Now the value of 'z' will be XORed along with the value of 'y'
- **Step 4**:- Store the obtained value in 'z'
- **Step 5**:-Now the value of 'z' have the result of multiplication.
- **Step 6**:- After matrix multiplication, XOR the value 'z' by $(99)_{10}$.

This will generate the following S-box



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

Figure 1:- S-Box for AES

Phase 2: Static S-Box

After obtaining the key matrix every fragment of the key expansion is under constant working state. Without waiting any performance improvement of the system can be reached. Key expansion is done in two parts. First part is responsible for calculating the part before the S-box and the second part takes responsibility of calculating the data passes after passing through S-box, but the issue still exists. It also produces multi-input and disordered issues and extends the design space requirements. Through the analysis, the size of the s-box is fixed to improve the performance. By applying new S-box design in short groups the anti-square attacking capability of the system can be improved. Along with this, the use of new S-box can extend the spread of the system. By providing conditions such as suitable memory space and operating speed, transforming the size of S-box or operating area of shift row can lower or remove the symmetry while the square attacking occurs and also upgrade the anti-square attacking ability of the AES in small sets. Along with this the security and the popularity of the AES encryption is increased.[31]

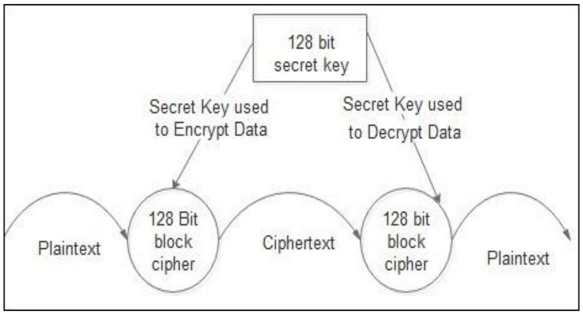


Figure 2:- DFD of AES algorithm in action for text encryption and decryption.

Phase 3:- Segmentation and Validation Algorithm

in this phase, the AES algorithm is collaborated with f conventional data segmentation and validation algorithm. This could help in validating the data size corresponding to the input data size; as a result the speed of encryption and decryption will be increased. Generally, if the test contains few amounts of data, the AES algorithm will be applied to encrypt or decrypt the data. But if the test contains large amount of data, the segmentation algorithm is applied prior to AES algorithm and then encryption and decryption will be done.[32]

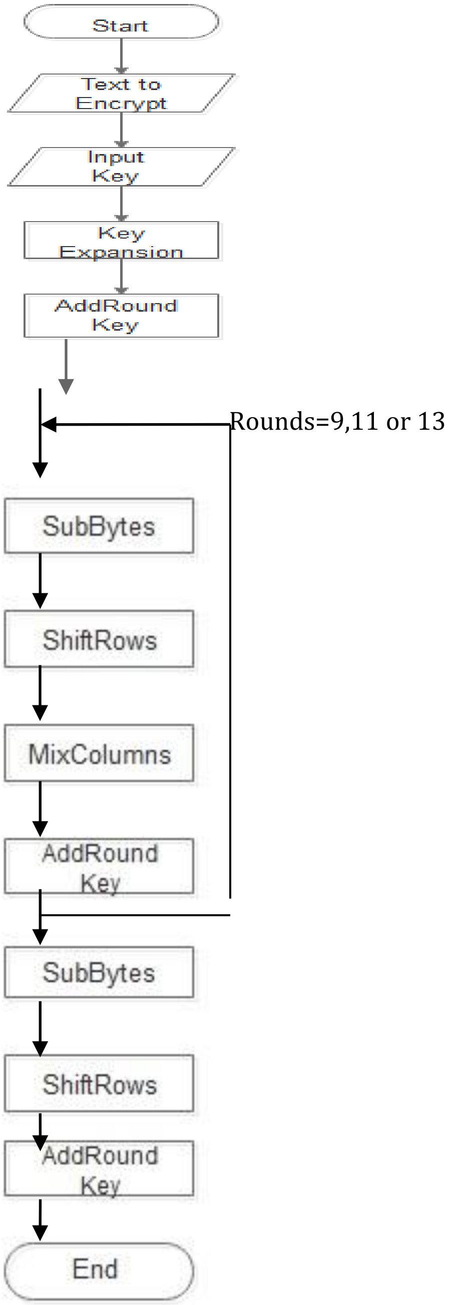


Figure 3:- Flowchart of AES

Hence, the speed to encrypt or decrypt data is fast and near to the level best of AES algorithm speed. This process has added the robustness and flexibility to the AES algorithm. Furthermore, the segmentation algorithm is carried prior to encryption and after the AES decryption while transmission. For more improvements the design divides the nine rounds into three parts, which means every three rounds will be processed as one block and three blocks will complete the whole nine rounds. This method is termed as the pipeline. Pipelining will increase the operating speed of the entire system. There will be no delay between any two blocks connected, and this will save the time for data transmission.[33]

3.1 Proposed Algorithm

The proposed AES is the improved form of existing AES algorithm. In proposed AES algorithm, to encrypt large amount of data, segmentation is done before encryption and after the decryption while transmission. The key expansion is also done to improve the security of the AES. Moreover, the nine rounds is completed in three blocks. This process is called pipelining which increase the operating speed of the entire system. The algorithm for the proposed AES is as follows:-

- **Step 1**:- Input Data Matrix (d).
- **Step2**:- Data Matrix Validation →validate(d)→d_M
- **Step3**:-Data Matrix Segmentation→segment((d_M))→d_m^i
- **Step 4**:- Input Security Key(S_k)
- **Step 5**:- Key Expansion(S_k)
- **Step 6**:- Initial Round→AddRoundKey (S_k)
- **Step7**:- Rounds→For Loop
  - SubBytes (d_m^i)
  - ShiftRows (d_m^i)
  - MixColumns (d_m^i)
  - AddRoundKey(d_m^i)
- **Step 8**:- Rounds→End For Loop
- **Step 9**:-Final Round→MixColumns (False)
  - SubBytes(d_m^i)
  - ShiftRows (d_m^i)
  - AddRoundKey (d_m^i)
- **Step 10**:- Data Matrix Merger→merge(d_m^i)→dE_M
- **Step11**:-Data Matrix Reverse Validation--rvalidation(dEM)→dE

To encrypt 128 bit blocks of data. Data is fed as an input to the system. The proposed AES is combined with validation and segmentation algorithm. So the created data matrix (d) will be validated. As the amount of data to be entered into the system is validated using validation algorithm. After this, matrix will be segmented (d_M) into fragments.

This segmentation is done to increase the operating speed of the system. Now the secret key (S_k) is input which is used to encrypt or decrypt the data. After inputting the secret key, key expansion is done. This key expansion will make the AES algorithm more secure. Now the initial round AddRoundKey (S_k) will be performed. The nine rounds are divided into three parts, means every three parts will be processed as one block and these three blocks will complete the all nine rounds. After the completion of rounds the data matrix will be merged (dE_m) and then data matrix reverse validation will be done. At the last we will get encrypted text.

Moreover, the decryption of the AES algorithm is more complex and consumes more time than the encryption. So after studying some books, papers and websites, two practical solutions are found: decomposing the changes of columns to diminish the numbers of times and constructing some forms. Based on reducing of the storage space, these two-decryption optimal algorithms process on the basis of the columns changing that makes the programming smaller than the original one and saves much more time.[34]

To perform the encryption, AES encryption algorithm is used to hide the image details of hidden object. The AES and Blowfish algorithms are the two popular, secure and robust for encryption algorithms, because these two gives the best encryption security. Out of these two algorithms, the conclusion was derived that the blowfish encryption algorithm is regarded the fastest one among the AES by a marginal difference. In the proposed model, the advanced encryption algorithm (AES) is depicted in a customized way to work with images in MATLAB environment. The algorithm code is developed to perform various rounds of encryption. The encryption algorithm is used here to conceal the image details and to develop a new image with dizzy image details. The image details are made hidden in disordered way to create a new image with fewer numbers of details. The image is not made completely unreadable because it causes the hacker to crack into the encryption, whereas a low resolution less detail encryption can be easily mistaken as a bad image. The decryption process is the reverse process, which is used to obtain the genuine image by using the reverse engineering of the cryptographic process on the receiver's end. For the decryption, user has to enter the identical key as it was entered on the sender's side while encrypting the image. The decryption operation returns the full resolution original image from the encrypted image once the process is complete. The image encryption using advanced encryption algorithm process has been listed.[35]

In this paper, focus is done in improving the security and performance of the AES. In order to improve the performance, AES algorithm can be used in parallel manner to execute operations.AES algorithm will be also modified for its source code bottlenecks and this will also help in the performance of the AES. The security of the AES will be improved by applying sine, cosine and tangent functions after performing the rounds to make the encrypted data more secure. In the first step we will input key and generate step key using secondary key expansion. This key will help in the encryption and decryption of the data. Below is the UML (Unified Modeling Language) to explain the encryption and decryption process.

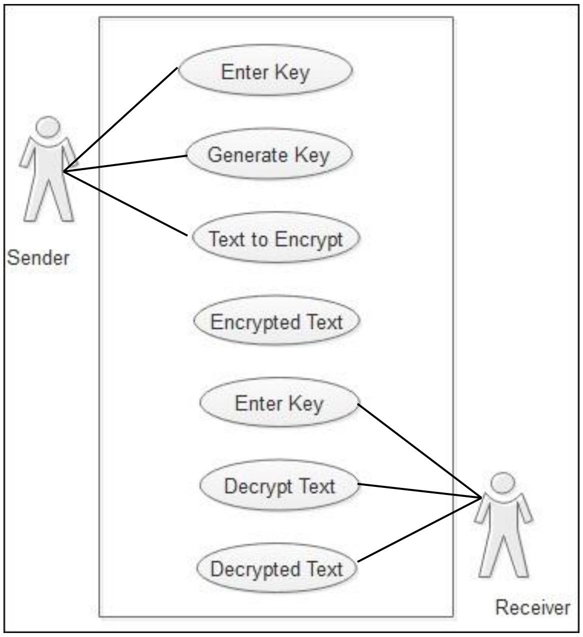


Figure 4:- Use Case Diagram of Proposed AES.

In Use Case Diagram, the sender will enter a secret key and then key will be generated. Now the text to be encrypted is entered and as a result the encrypted text will be generated. On the receiver side, the receiver uses the same key to decrypt the text and will get the original text.

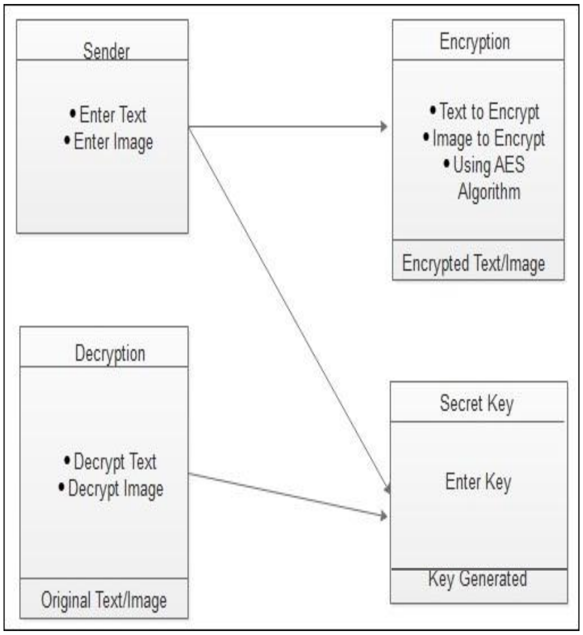


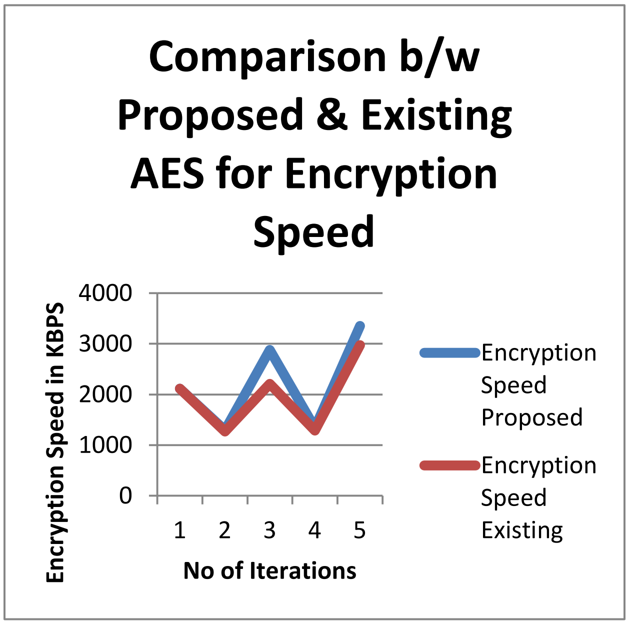
Figure 5:- Class Diagram of Proposed AES.

In class diagram, there are two entities sender and receiver. The sender will send the text or image to encrypt, this encryption is done using AES algorithm. Then a secret key will be generated used in the encryption process. At the receivers end the text or image will be decrypted with the help of the same secret key.

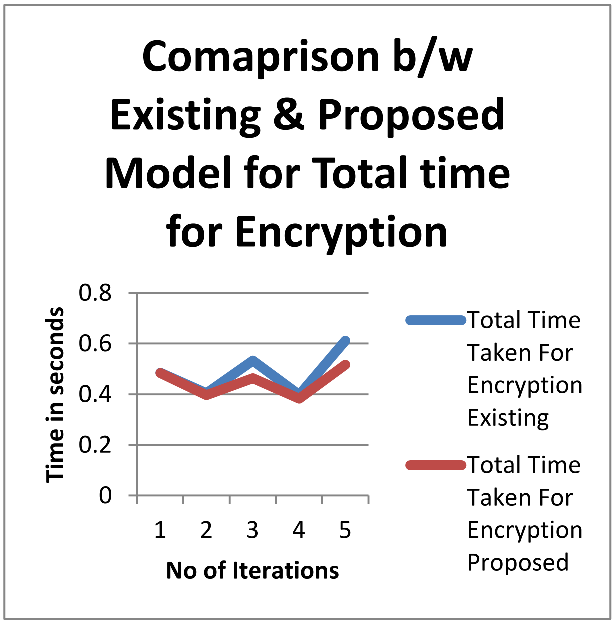
3. Results and Discussions

This section evaluates the improved version of the AES algorithm. In this, speed of encryption and decryption is increased within less time. Performance and security of AES is improved as compared to the existing AES algorithm. Evaluations are done on a single core of an Intel Core i3-2400 CPU at 3100 MHz, and unexceptionally over 1000 repetitions. Our conclusions are listed in Tables and Graphs. It is seen that while the initialization overhead mainly has a enormous effect on the performance, this effect fade out already at messages of around 256-1500 bytes. Due to the fast execution of the proposed AES algorithm it is proved better than the existing AES algorithm. The proposed AES attains nearly excellent performance beginning from 512 bytes message length due to its capability of programming structure which allows it to completely employ the improved multiple encryption standards and validation for its initialization overhead. The proposed AES performs superior than the existing AES when it is formulated with block size of 128 bit and static S-box implementation. Besides, the validation process has been included to assign more flexibility and robustness to the proposed algorithm.

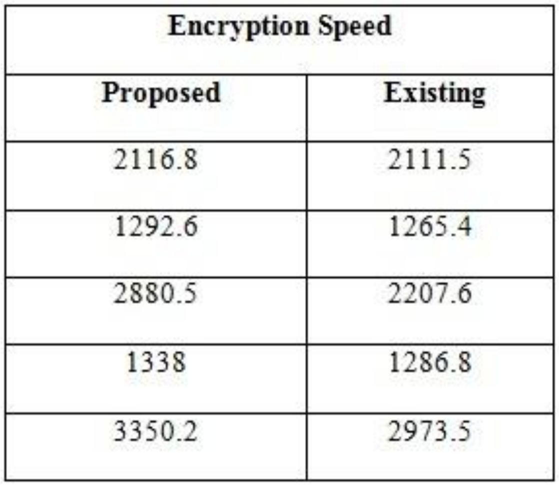
For testing the performance of the proposed and the existing algorithm, different sizes of data has been employed. The conclusions have showed the effectiveness of the time and encryption-decryption speed for proposed algorithm. The performance of the proposed algorithm has been analyzed on the Index Core i3 CPU with 2GB RAM. The encryption speed has been recorded between 1338 and 3350 Kbps. The standard value recorded for the encryption speed has been noted at the 2152.8 Kbps and the decryption speed has been noted between 127930.7 Kbps and 753842.7, though the average decryption speed has been noted at 343953.44 Kbps speed. The encryption and decryption speeds have proved the success of the proposed algorithm on testing data. The elapsed time for encryption process and decryption process has also been noticed. The average size of data when transformed to the double type has been noted at 1024 Kbps.



(a) Encryption Speed comparison between Proposed and existing algorithm.

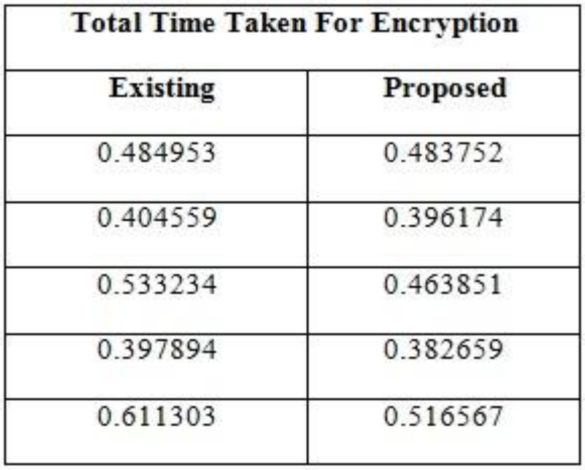


(b) Comparison between Existing and Proposed model for total time taken for encryption.



Encryption Speed	
Proposed	Existing
2116.8	2111.5
1292.6	1265.4
2880.5	2207.6
1338	1286.8
3350.2	2973.5

(a) Table Encryption Speed between Existing and Proposed AES.

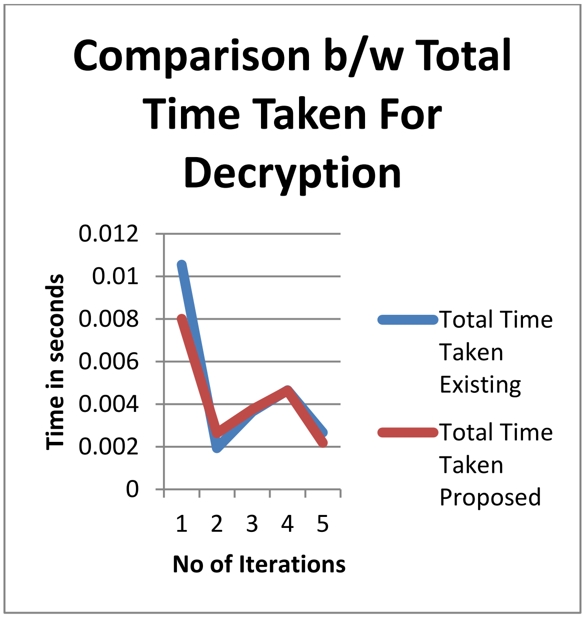


Total Time Taken For Encryption	
Existing	Proposed
0.484953	0.483752
0.404559	0.396174
0.533234	0.463851
0.397894	0.382659
0.611303	0.516567

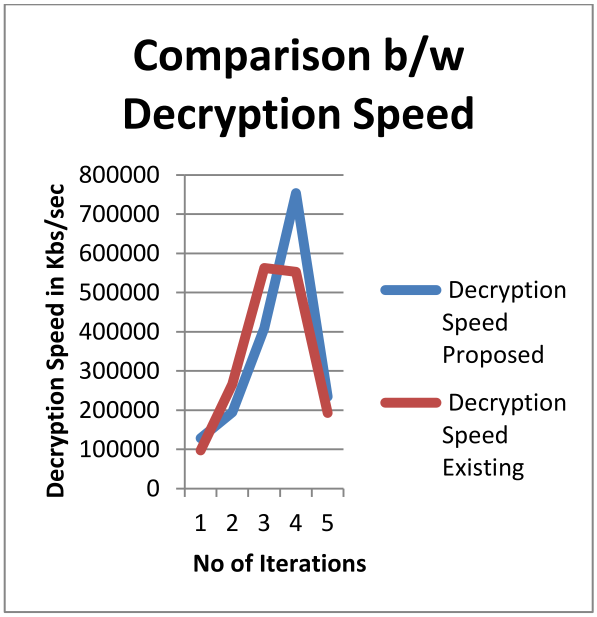
(b)Table showing comparison between Total time taken for encryption.

The Graph (a) and Table (a) is showing the results acquired from the existing and proposed AES implementation for Text and image data. The table is representing the encryption speed on the basis of the several data sizes. Rotating the iterations for 64 bytes of data creates the test over the variable data sizes. The data of 64 bytes has been iterated for 128, 256, 512, 1024, 2048 and 4096 times to achieve the data sizes of 64 kb, 128 kb, 256 kb, 512 kb, 1024 kb, 2048 kb and 4096 kb, respectively.

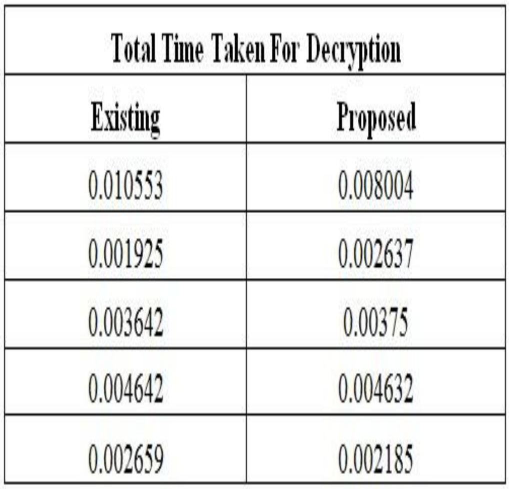
The Graph (b) and Table (b) is showing the results acquired from the existing and proposed AES implementation for Text and image data. The table is showing the elapsed time for encryption on the basis of the various data sizes. Rotating the iterations for 64 bytes of data creates the test over the variable data sizes. The data of 64 bytes has been iterated for 128, 256, 512, 1024, 2048 and 4096 times to achieve the data sizes of 64 kb, 128 kb, 256 kb, 512 kb, 1024 kb, 2048 kb and 4096 kb, respectively.



(c) Comparison between Total Time Taken For Decryption

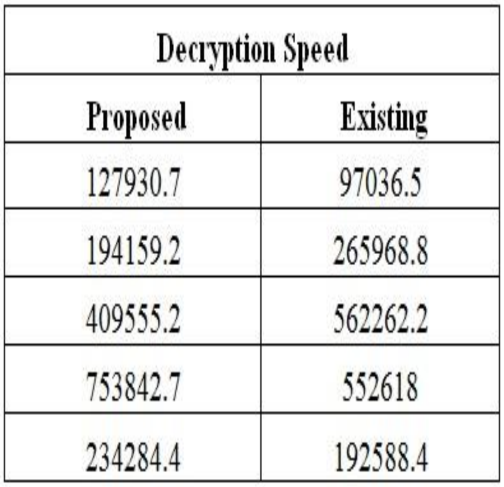


(d) Comparison between Decryption Speed



Total Time Taken For Decryption	
Existing	Proposed
0.010553	0.008004
0.001925	0.002637
0.003642	0.00375
0.004642	0.004632
0.002659	0.002185

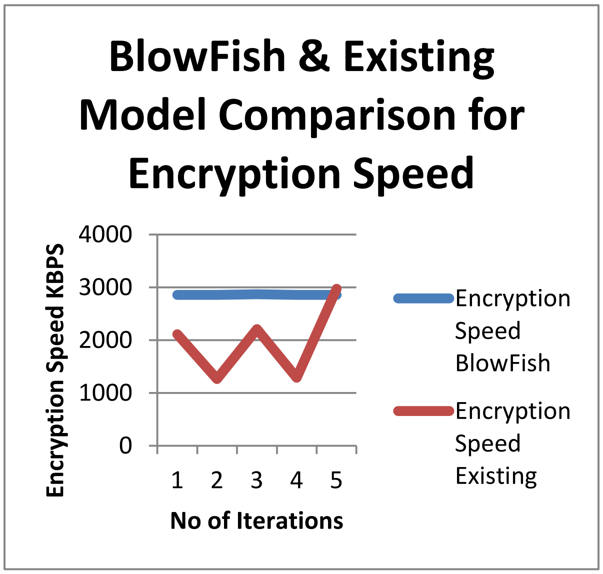
(c) Table Showing Time taken for Decryption between Proposed and Existing.



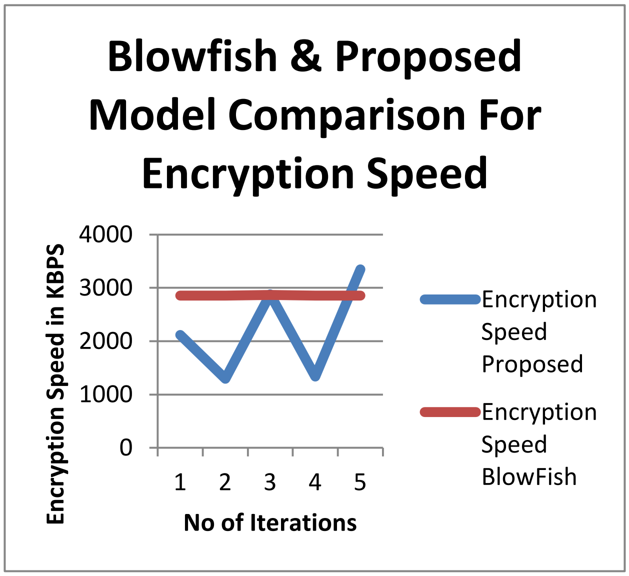
Decryption Speed	
Proposed	Existing
127930.7	97036.5
194159.2	265968.8
409555.2	562262.2
753842.7	552618
234284.4	192588.4

(d) Decryption Speed comparisons between Proposed and Existing.

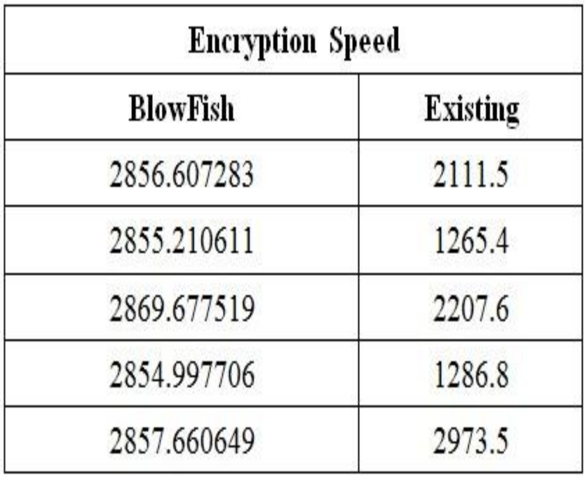
The subsequent Graph (c) and Table (c) is depicting the results acquired from the existing and proposed AES implementation for Text and image data. The Table is representing the elapsed time for decryption on the basis of the several data sizes. Rotating the iterations for 64 bytes of data creates the test over the variable data sizes. The data of 64 bytes has been iterated for 128, 256, 512, 1024, 2048 and 4096 times to achieve the data sizes of 64 kb, 128 kb, 256 kb, 512 kb, 1024 kb, 2048 kb and 4096 kb, respectively.The subsequent Graph (d) and Table (d) is depicting the results acquired from the existing and proposed AES implementation for Text and image data. The table is showing the decryption speed on the basis of the various data sizes. Rotating the iterations for 64 bytes of data creates the test over the variable data sizes. The data of 64 bytes has been iterated for 128, 256, 512, 1024, 2048 and 4096 times to achieve the data sizes of 64 kb, 128 kb, 256 kb, 512 kb, 1024 kb, 2048 kb and 4096 kb, respectively.



(e) BlowFish & Existing Model Comparison for Encryption Speed

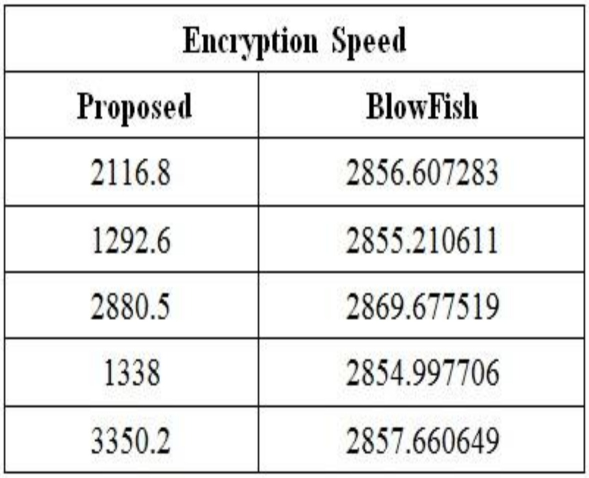


(f) Blowfish & Proposed Model Comparison for Encryption Speed



Encryption Speed	
BlowFish	Existing
2856.607283	2111.5
2855.210611	1265.4
2869.677519	2207.6
2854.997706	1286.8
2857.660649	2973.5

(e) Table Showing Encryption speed comparison between Blowfish and Existing AES.



Encryption Speed	
Proposed	BlowFish
2116.8	2856.607283
1292.6	2855.210611
2880.5	2869.677519
1338	2854.997706
3350.2	2857.660649

(f) Table showing Encryption speed comparison between Blowfish and Proposed AES.

The following table is showing the results obtained from the existing AES and BlowFish implementation for Text and image data. The table is representing the encryption speed on the basis of the various data sizes. Rotating the iterations for 64 bytes of data creates the test over the variable data sizes. The data of 64 bytes has been iterated for 128, 256, 512, 1024, 2048 and 4096 times to achieve the data sizes of 64 kb, 128 kb, 256 kb, 512 kb, 1024 kb, 2048 kb and 4096 kb, respectively. The following table is showing the results acquired from the BlowFish and proposed AES implementation for Text and image data. The table is showing the encryption speed on the basis of the various data sizes. Rotating the iterations for 64 bytes of data creates the test over the variable data sizes. The data of 64 bytes has been iterated for 128,256, 512, 1024, 2048 and 4096 times to achieve the data size of 64 kb, 128 kb, 512 kb, 1024 kb, 2048 kb and 4096 kb respectively.

The rapid execution of the AES algorithm for software systems has been witnessed it as the one of the best encryption algorithm. The users in the user interface have examined the AES algorithm with five number of text messages/images entered.[8] The user message is demonstrated and separated according to the allowed block size. The text message is when entered is in the form of string and relates to the character data type. The presented AES algorithm authorizes the input in the arrangement of double data type only. All tables represent the size of the text message in different data types at diverse stages of the encryption and decryption process.

The proposed algorithm has been proved to be way faster than the current AES algorithm. The current algorithm is taking almost 7-8 times slower than the proposed algorithm. The proposed algorithm has been proved to be effective for both image and text data.

4. Conclusion

In this paper, an improved AES has been proposed which will be more secure and good in performance as compared to existing AES. The data to be encrypted is pipelined to increase the speed and time to encrypt the text or image data. AES is combined with Validation and Segmentation. Key Expansion is done to make the data more secure. Also, the blowfish is compared with this improved version of AES. But as a result the blowfish is fast and more secure encryption algorithm as compared to the proposed AES. The future scope of this project can be that the AES can be made more secure and reliable and can be made faster and good than blowfish algorithm.

References

[1] William August Kotas, "Brief History of Cryptography", International Journal of Dairy Science and Technology (IJDST), Vol. 10, No. 8,pp.183-197,2000.

[2] David Kahn, "History of Cryptography", SANS Institute Infosec Reading Room, Vol. 13,No.22,pp.951-961,2001.

[3] Nicholas G.McDonald, "Past and Present Methods of Cryptography and Data Encryption", University of UTAH, Vol 4,No.25,pp.156-168,2002.

[4] Garcy C.Kessler, "An Overview of Cryptography", Handbook on Local Area Network, Vol.10, No.24, pp-234-240, 2016.

[5] Roger A. Prichard, "History of cryptography", Global Information Assurance Certification Paper (GIAC), Vol.18, No.22, pp-356-367, 2002.

[6] S.J. Sharma, "The Art of Cryptography: From Ancient Number System to Strange Number System", International Journal of Application or Innovation in Engineering and management (IJAIEM), Vol.2, No.4, ISSN 2319-4847, 2013.

[7] Mohammed Abutaha, Mousa Farajallah, Radwan Tahboub, Mohammad Odeh, "Survey Paper: Cryptography Is the Science of Information Security", International Journal of Computer Science and Security (IJCSS), Vol.5, No.3, 2011.

[8] Kartalopoulos,Stamatios V."A Primer on Cryptography in Communications." Institute of Electrical and Electronics Engineers (IEEE) Communications Magazine,pp. 146-51,2006.

[9] Hassan Mathkour, Ghazy Assassa, Al-Muharib, A. Juma'h, "A Secured Cryptographic Messaging System",International Conference on Machine Learning and Computing (ICMLC), Vol.3,No.5,2009.

[10] Simon Singh, "Classical Encryption", Institute of Electrical and Electronics Engineers (IEEE), Vol.6, No.8, 2010.

[11] Ahmed Al Vahed, Haddad Sahhavi,"An Overview of Modern Cryptography", World

Applied Programming (WAP) Journal, Vol.1, No.1, pp-55-61, ISSN: 2222-2510, 2011.

[12] Rodriguez-Henriquez,F.Saqib, "Cryptographic algorithms",Springer,ISBN:978-0-387-33883-5,2007.

[13] Jonathan Katz and Yehuda Lindell Chapman & Hall, “Introduction to Modern Cryptography”, International Association for Cryptologic Research (IACR), ISBN: 1-58488-551-3, 978-1-584-885-511,2011.

[14] Dr. Prerna mahajan and Abhishek Sachdeva, "A Study of Encryption Algorithms AES,DES and RSA Security" ,Global Journal of Computer Science and Technology Network, Web and Security, Vol. 13,No.15,ISSN:0975-4172,2013

[15] Douglas Selent, "Advanced Encryption Standard", Rivier Academic Journal, Vol. 6, No. 2,2010

[16] M.Pitchaiah, Philemon Daniel, Praveen, "Implementation of Advanced Encryption Standard Algorithm", International Journal of Scientific & Engineering Research (IJSER), Vol.3, No.3, ISSN 2229-5518, 2012.

[17] Ritu Pahal and Vikas Kumar, "Efficient Implementation of AES" ,International Journal of Advanced Research in Computer Science and Software Engineering,Vol.3,No.7,ISSN 2277 128X,2013

[18] Wang, Xing-Yuan, Sheng-Xian Gu, and Ying-Qian Zhang. "Novel image encryption algorithm based on cycle shift and chaotic system." Optics and Lasers in Engineering Vol.6, No.8,pp. 126-134,2015

[19] Prof.CristofPaar, "Applied cryptography and data security”, Cryptography and Information Security (CRIS) Group, vol.2 No.5, 2005.

[20] Creighton Hager, "Performance and energy efficiency of block ciphers in personal digital assistants”, Institute of Electrical and Electronics Engineers (IEEE), Vol.10, No.12, pp. 127 – 136, 2005.

[21] Gary Kessler, "An Overview of Cryptography”, Handbook on Local Area Networks (HLAN), Vol. 1, No.3, pp-278-285, 2006.

[22] Alaa Yasen Taqa and Aos Alaa Zaidan," New framework for high secure data hidden in the MPEG using AES encryption algorithm” International Journal of Computer and Electrical Engineering (IJCEE),Vol. 1, No.5, pp. 566-571, 2009.

[23] Mohammadi, "A high level security mechanism for Internet polls”, Signal Processing Systems (ICSPS), 2nd IEEE, Vol. 3, No.5, pp. V3-101 - V3-105, 2010.

[24] Pitchaiah, Philemon and Praveen, "Implementation of Advanced Encryption Standard Algorithm", International Journal of Scientific & Engineering Research (IJSER), Vol. 3, No.3, ISSN: 2229-5518, 2012.

[25] Navita Agarwal, “An Efficient Pixel-shuffling Based Approach to Simultaneously Perform Image Compression, Encryption and Steganography", International Journal of Computer Science and Mobile Computing (IJCSMC), Vol.2, No.2, pp.376 – 385, 2013.

[26] MilindMathur, "Comparison between DES, 3DES, RC2, RC6, BLOWFISH and AES”, National Informatics Center Network NICNET, Vol. 1, No.3, pp. 143-148, 2013.

[27] Sasan Adibi,“A low overhead scaled equalized harmonic-based voice authentication system”, Telematics and Informatics, Vol. 31, No. 1, pp. 137-152, 2014.

[28] Abdouli et al.,” Survey on computationally hard problems and their applications to cryptography”, Internet Technology and Secured Transactions (ICITST), IEEE, Vol.12, No.14, pp.46 – 52, 2011.

[29] Verma,” Peformance analysis of data encryption algorithms” International Conference on Electrical and Computer Technologies (ICECT), 3rd IEEE, Vol. 5, No.7, pp. 399 – 403, 2011.

[30] Chrisrophe De Canniere, Alex Biryukov and Bart Preneel, "An Introduction to Block Cipher Cryptanalysis",Institute of Electrical and Electronics Engineers(IEEE), Vol.94, No.2, ISSN:0018-9219, 2006.

[31] Neal R. Wagner, "The Laws of Cryptography: Advanced Encryption Standard: S-Boxes", International Organization for Standardization, Vol.89, No.5, pp. 067-456, 2001.

[32] Jasmeet Singh, Harmandeep Singh, "Design and Development of a Rapid AES based Encryption Framework",International Journal of Engineering Research & Technology(IJERT),Vol.3,No.10,ISSN:2278-0181,2014.

[33] Lawrence E. Bassham,"The Advanced Encryption Standard Algorithm Validation Suite", National Institute of Standards and Technology Information Technology Laboratory Computer Security Division, Vol.14, No.06, pp.789-981, 2002.

[34] Jie Cui1,Liusheng Huang,Hong Zhong, Chinchen Chang and Wei Yang,"AN IMPROVED AES S-BOX AND ITS PERFORMANCE ANALYSIS",International Journal of Innovative Computing, Information and Control, Vol.7, No.5(A), pp.2291-2302, ISSN 1349-4198, 2011.

[35] Nagendra and Chandra Sekhar, "Performance Improvement of Advanced Encryption Algorithm using Parallel Computation",(IJSEIA), Vol.8, No.2, pp.287-296, ISSN: 1738-9984, 2014.