RESEARCH ARTICLE OPEN ACCESS

Comparative Analysis of Parallel AES Algorithm with Pipelined AES Algorithm

Tannu Bala [1], Yogesh Kumar [2]
Department of Computer Science
PTU/ Bhai Gurdas Institute of Engineering & Technology
Sangrur - India

ABSTRACT
AES (Advance Encryption Standard) algorithm is very popular and robust encryption algorithm out of all other available encryption algorithms. AES is considered as highly secure and almost unbreakable encryption standard. AES carries a major drawback of taking high execution time and lower throughput. AES has comparatively lower throughput and high time for all kinds of data. AES algorithm will be also modified for its source code bottlenecks. It is very important to remove the bottlenecks from the execution flow of the algorithms to improve their performance. AES can be possibly modified in some ways for its performance enhancements to improve its performance. According to our studies, we have found some possible options to improve the performance of AES algorithm.
Keywords:- AES Algorithm, Parallel Data Transition, encryption speed, decryption speed, encryption Time, decryption Time.

I. INTRODUCTION

It is going to be good to understand the concept of information. To understand cryptography term, an issues related to information security is necessary to be clear. A set of mechanisms and protocols had created and based on this physical documented information was secured. Just by applying mathematical algorithms and protocols we do not achieve security, to get the desired result we have to require obedience of laws and procedural techniques. For example, sealed envelope shows the privacy of letter delivered by an accepted mail service [1].

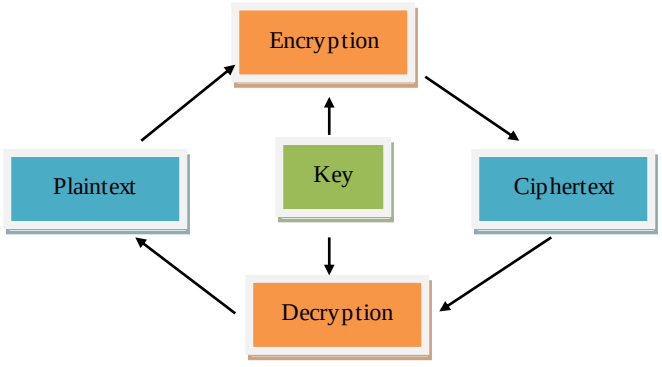

Fig 1: working process of Cryptographic algorithm

Cryptography is necessary in data and telecommunications, when communication is done through any un-trusted medium, which may be any type network, specially the Internet. Along with user authentication cryptography is also used for the protection of data from thief. Basically three types of cryptographic schemes are used to achieve this goal: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions. In all cases, plaintext is referred as input data or initial unencrypted data. This encrypted information is further known as cipher-text, which will later decrypt into plaintext [2]. With change of time the way to store information has not changed. In previous days, paper was used to store information and transmit, but currently technology enhanced, information domiciled on magnetic media (CDs and Hard Disks) and is transmitted via wireless and telecommunications systems. This gravely modification makes copy and alter information terribly easier. Multiple identical copies of same information are generated and keep electronically. With information on paper, this can be rather more troublesome.

The knowledge that is keep and transferred through electronic media or channel needs a lot of security. In securing the information, signature is the one among the most and basic technique (tool). Signature is that the building blocks for several different services like non-repudiation, information origin authentication and identification. Signature is utilized to identify, authorize, and validate the individual person therefore it's to be distinctive. With the help of electronically stored information the construct of a signature has got to be updated time by time for security of the knowledge [2]. If we have made a will or made a document, and signed it, this means it is your responsibility, it is - say for example, it is a kind of authorization that you have a cheque and you sign over it- in other words you say that; it is my signature, that I am permitting this transaction, and I have knowledge of this transaction [3].

Authentication is also a very important goal. Often, digital signatures are used to obtain the goals of authentication. Computer science practice and mathematical theory is the main base of Modern; these cryptographic algorithms are designed for computational hard problems, in practice these algorithms are very hard to break. These algorithms may be easy to break theoretically, but it is infeasible to break by any practical means.

Today's practical work use combination of symmetric algorithms together with public-key algorithms which is known as hybrid schemes. In hybrid scheme, symmetric keys distribute by Asymmetric algorithm known as a session key. Symmetric algorithm provides bulk encryption.

Cryptographic algorithm acts as a resistance to any unauthorized person who want to access yours sensitive information. To measure and counter different attacks cryptography used as a tool. It is a method in which only authorized parties can read and process personal data. For security purposes cryptography use Encryption and Decryption techniques. All algorithms are key based algorithms. On the sender side information is coded by using encryption opposite to receiver side where decryption is used for decoding that information. This encryption-decryption process gives full security to sensitive information. Some common algorithms are DES, RSA, BLOWISH.

II. ALGORITHM

Across the world **AES** is adopted by many organizations. Ranging from smart cards to big servers applications AES is used just because of its simplicity, flexibility, easiness of implementation, and high throughput. Two cryptographers develop AES, Joan Daemen and Vincent Rijmen, hence also referenced as **Rijndael** encryption algorithm. With increasing speed of microprocessor chips and increasing technology DES (the Data Encryption Standard) become obsolete. A new Encryption standard, called the **A**dvanced **E**ncryption **S**tandard was established by United States National Institute of Standards and Technology (NIST), in 1997, to replace DES as the Federal Information Processing Standard (FIPS). In October 2002, **Rijndael** a block cipher algorithm was accepted as the new Advanced Encryption Standard.

With variable block and key lengths Rijndael is an iterated block cipher. The block length and the key length can vary and each of 128, 192, or 256 bits in size. The block and the intermediate cipher can be envisioned as a two-dimensional array of four rows called the State. The number of columns varies depending on the bit length. Block size of 128-bit AES id shown in figure.

In Rijndael, each operation is performed either on single byte or on 4-byte word. Key is also viewed same as this format. Depending on the block size, plaintext gives as input to the cipher, and is one-dimensional array of 16, 24 or 32 bytes. In state these bytes are mapped in column order [4].

Rijndael is an iterative algorithm. A different key derived from initial key is used in each of the iterations, called a round. The number of rounds depends on the key. The following table gives the number of rounds to be performed based on the block length (BL) and key length (KL) in terms of bits [4].

O1	O5	O9	O13
O2	O6	O10	O14
O3	O7	O11	O15
O4	O8	O12	O16

Fig 2: 128 bit AES Block [4]

ByteSub Transformation: This operation is a nonlinear byte substitution. According to the substitution box each byte from the input state is replaced by another byte. On each cells of the State this transformation works independently. This transformation works in two parts. First, the multiplicative inverse of the byte is calculated, followed by an affine transformation [4].

ShiftRow Transformation: All of the four rows independently go through from this transformation. With the help of different offset each row is cyclically shift left expect the first row. By using the block length offsets of each row are determined. In case of Decryption, to neutralize the effect, the rows are shifted back, called InvShiftRow. That is, the rows are cyclically shifted left with offset equal to number of columns of State minus the offset for Encryption [4].

MixColumn Transformation: On each column of the State this transformation works independently. A polynomial is the single column of the State on which this transformation works. [4]

Round Key Addition: In this transformation, the Round Key is combined with the State. This addition in GF (2^8) is a simple performed with bit wise XOR. The round key and State both have same length. It is derived from the initial cipher by means of Key Schedule. [4]

III. PREVIOUS WORK

There exist many presentations of AES algorithms in literature. Some of them will be briefly introduced here. In 2014 Abhilasha Naidu describe AES algorithm to increase the throughput of the algorithm. Pipelined concept is used to increase the throughput of algorithm. In 2014 Jasmeet Singh Design the New Rapid AES algorithm. The result has proved

INDEX	File Size (Kb)	Proposed Algorithm		Existing Algorithm	
		Encryption Time (seconds)	Decryption Time (seconds)	Encryption Time (seconds)	Decryption Time (Seconds)
1	512.00	43.215658	26.394590	91.117041	48.474545
2	1183.710938	103.01652	58.939383	205.968018	107.74608
3	1215.500000	105.453487	58.499072	217.847958	116.822427
4	548.437500	46.369796	23.156968	91.327312	48.940831
5	3331.437500	257.835222	162.116017	613.862835	311.053233
6	394.523438	32.846024	19.811458	69.404918	37.206873
7	395.507813	39.884092	23.377744	74.014128	39.198705
8	200.000000	20.329600	11.774322	38.268508	20.252559
9	394.148438	38.698187	22.374805	72.725517	38.543829
10	395.507813	29.579611	17.424436	81.369108	42.894914

that Rapid AES performed better than the existing AES on image data type. The Rapid and existing AES algorithms has been recorded for their encryption speeds, elapsed time for encryption, elapsed time for decryption, decryption speeds, etc. In 2013 Milind Mathur compares different symmetric algorithms (DES, 3DES, Blowfish and AES). He was concludes that in the case of performance, blowfish is better than all other algorithms and in the case of changing data type AES is better. In 2013 Navita Agarwal combines three techniques compression, encryption and steganography on the digital image data. This combined approach hides the existence of secret image making it almost impossible to snoop in the network, provides extremely high security and consumes very less space. In 2005 T. R. Hager discusses the performance of various encryption algorithms on various kinds of data. This research has proved that blowfish outperforms all other encryption algorithms. Blowfish is unbreakable and fast encryption algorithm than others.

IV. EXPERIMENTAL RESULTS

Proposed AES algorithm has been designed for long data encryption. User may insert data with any number of bits to be encrypted by AES algorithm. Proposed AES algorithm has divide this plain text into four 128 bit modules and then each transition (Sub Byte, Shift Row, Mix Column and Add Round Key) is performed on that plain text. The proposed algorithm has been designed with the main motive of increasing the speed of the encryption and decreasing the time consumption by the encryption of the data.

TABLE I
the table displaying the results of Proposed AES implementation on dataset of 10 images (Encryption/Decryption Time)

TABLE III
the table displaying the results of Proposed AES implementation on dataset of 10 images (Encryption/Decryption Time)

INDEX	File Size (Kb)	Proposed Algorithm		Existing Algorithm	
		Encryption Speed (Kbps)	Decryption Speed (Kbps)	Encryption Speed (Kbps)	Decryption Speed (Kbps)
1	512.00	11.146201	19.026947	5.619146	10.562245
2	1183.710938	11.490496	20.083531	5.747062	10.986115
3	1215.500000	11.526409	20.778108	5.579580	10.404680
4	548.437500	11.827473	23.683476	6.005186	11.206134
5	3331.437500	12.920801	20.549712	5.427006	10.710184
6	394.523438	12.011300	19.913902	5.684373	10.603510
7	395.507813	9.916430	16.918134	5.343680	10.089818
8	200.000000	9.837872	16.986117	5.226229	9.875295
9	394.148438	10.185191	17.615726	5.419672	10.225980
10	395.507813	13.370961	22.698457	4.860663	9.220389

By using AES Algorithm, we can encrypt and decrypt the images. Total 10 different images (having different sizes) are taken to perform encryption and decryption. These Images are encrypted with Existing AES and Proposed AES and

Calculate the Encryption and Decryption time, Encryption and decryption speed. Based on these results comparison of both the Existing and Proposed AES Algorithm has been done and based on this we draw the graph.

These above tables give the complete data regarding the total data size of images that is taken for encryption and decryption of the data. Then calculate the time taken for encryption and decryption and compare this time taken by proposed parallel algorithm and existing pipelined algorithm. This result shows that proposed algorithm is very fast as compare existing algorithm.

The fast implementation of the AES algorithm for software systems has been proved it as the one of the best encryption algorithm applicants. The users in the user interface have tested the AES algorithm with ten number of text messages/images entered. The user message is validated and segmented according to the permitted block size. The text message is when entered is in the form of string and belongs to the character data type. The proposed AES algorithm authorizes the input in the form of double data type only. All tables represent the size of the text message/Image in different data types at various stages of the encryption and decryption process.

TABLE IIIII
the table displaying the results of Proposed AES implementation on dataset of 10 text data (Encryption/Decryption Time)

INDEX	File Size (Kb)	Proposed Algorithm		Existing Algorithm	
		Encryption Time (Seconds)	Decryption Time (Seconds)	Encryption Time (Seconds)	Decryption Time (Seconds)
1	1024.000000	0.402803	0.006358	0.430444	0.005986
2	512.000000	0.362142	0.006329	0.410112	0.024290
3	1536.000000	0.467883	0.007165	0.458805	0.009713
4	2048.000000	0.521139	0.010303	0.531878	0.011643
5	3072.000000	0.619014	0.019533	0.615809	0.023051
6	5120.000000	0.800331	0.010641	0.823661	0.012002
7	4608.000000	0.761467	0.013321	0.755656	0.014766
8	4096.000000	0.714512	0.011660	0.720898	0.012403
9	6144.000000	0.933384	0.014003	0.929788	0.014861
10	8192.000000	1.140345	0.017176	1.140592	0.014763

TABLE IVV
the table displaying the results of Proposed AES implementation on dataset of 10 text data (Encryption/Decryption Time)

INDEX	File Size (Kb)	Proposed Algorithm		Existing Algorithm	
		Encryption Speed (Kbps)	Decryption Speed (Kbps)	Encryption Speed (Kbps)	Decryption Speed (Kbps)
1	1024.000000	2542.2	161050.9	2496.9	171058.7
2	512.000000	1413.8	80891.5	1531.6	21078.8
3	1536.000000	3282.9	214362.6	3347.8	158131.7
4	2048.000000	3929.9	198776.8	3850.5	175904.9
5	3072.000000	4962.7	157272.2	4988.6	133271.5
6	5120.000000	6397.4	481177.8	6216.2	426578.3
7	4608.000000	6051.5	345918.5	6098.0	312058.5
8	4096.000000	5732.6	351296.3	5681.8	330247.0
9	6144.000000	6582.5	438762.0	6608.0	413434.5
10	8192.000000	7183.8	476948.1	7182.2	554892.5

By using AES Algorithm, we can encrypt and decrypt the text data. Total 10 different text data (having different sizes) are taken to perform encryption and decryption. These data are encrypted with Existing AES and Proposed AES and Calculate the Encryption and Decryption time, Encryption and decryption speed. Based on these results comparison of both the Existing and Proposed AES Algorithm has been done and based on this we draw the graph.

V. CONCLUSIONS

An Advanced Encryption Standard algorithm has been presented to solve the high time consumption problem by using time and throughput parameters. The motive of the algorithm is to resolve the problem of high time consumption while encryption and decryption of data and images. The proposed algorithm has been proved to be way faster than the existing AES algorithm. The proposed algorithm is 7-8 times faster than the existing algorithm. The proposed algorithm has been proved to be efficient for both image and text data. Our conclusions are shortened in Tables and Graphs. One can see that while the initialization overhead generally has a huge impact on the performance, this effect starts to fade out already at messages of around 256-1500 bytes. A good performance level is achieved with AES algorithm.

FUTURE SCOPE

For the future improvement in AES algorithm, the results of the work done here give direction for further research. As AES algorithm is still slow as compare to Blowfish algorithm. The work of AES can be extended for other techniques and taking other parameters for better results as compare to blowfish. In future AES can be evaluated with more data taken as encryption and as decryption. The future work may focus on other parameters.

REFERENCES

[1] Alfred J. Menezes" Applied Cryptography" June 1996.

[2] Gary C. Kessler" An Overview of Cryptography", *HLAN*, ver. 1, Nov 2006.

[3] Prof. D. Mukhopadhyay" Cryptography and Network Security".

[4] Jasmeet Singh, Harmandeep Singh" Design and Development of a Rapid AES based Encryption Framework", *International Journal of Engineering Research & Technology (IJERT)*, Vol. 3 Issue 10, October- 2014.

[5] Abhilasha Naidu, A.Y. Deshmukh, Vipin Bhure "Design of High Throughput and Area Efficient Advanced Encryption System Core", *International Conference on Communication and Signal Processing, IEEE*, April 2014.*International Conference on Communication and Signal Processing, IEEE*, April 2014.

[6] Milind Mathur, Ayush Kesarwani" Comparison between DES, 3DES, RC2, RC6, BLOWFISH and AES", *Proceedings of National Conference on New Horizons in IT, NCNHIT*, vol. 1, pp. 143-148, 2013.

[7] Navita Agarwal, Himanshu Sharma "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, pp. 376 – 385, May 2013.

[8] CTR Hager, SF Midkiff, JM Park" Performance and energy efficiency of block ciphers in personal digital assistants", *Pervasive Computing and Communications, 3rd IEEE*, pp. 127 – 136, March 2005.

[9] Crs Bhardwaj "Modification of Des Algorithm", *International Journal of Innovative Research and Development*, vol 1 issue 9, Nov 2012.

[10] Thakur, Jawahar, and Nagesh Kumar. "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis."International journal of emerging technology and advanced engineering 1.2, 2011.

[11] Standard, Secure Hash. "The Cryptographic Hash Algorithm Family: Revision of the Secure Hash Standard and Ongoing Competition for New Hash Algorithms.", 2009.

[12] Geoff Hamilton" Cryptography and Number Theory".

[13] Dr. Prerna Mahajan, Abhishek Sachdeva" A Study of Encryption Algorithms AES, DES and RSA for Security", *Global Journal of Computer Science and Technology Network, Web & Security*, Volume 13, Issue 15 Version 1.0, 2013.

[14] Abhilasha Naidu, A.Y. Deshmukh, Vipin Bhure "Design of High Throughput and Area Efficient Advanced Encryption System Core", *International Conference on Communication and Signal Processing, IEEE*, April 2014.

[15] Dudhatra Nilesh, Prof. Malti Nagle "The New Cryptography Algorithm with High Throughput", *International Conference on Computer Communication and Informatics ICCCI*, pp. 03 – 05, Coimbatore, Jan. 2014.

[16] Quist-Aphetsi Kester, Laurent Nana, Anca Christine Pascu, Sophie Gire, J. M. Eghan, Nii Narku Quaynor "Feature Based Encryption Technique For Securing Forensic Biometric Image Data Using AES and Visual Cryptography", 2nd *International Conference on Artificial Intelligence*, 2014.