IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Issue-6 E-ISSN: 2347-2693

Security of Personal Data on Internet of Things Using AES

[1*]Sadiya Shakil and [2]Vineet Singh

[1,2] Department of Computer Science and Engineering, Amity University, Lucknow

www.ijcseonline.org

Received: May/26/2016 Revised: Jun/10/2016 Accepted: Jun/22/2016 Published: Jun/30/ 2016

Abstract-This paper includes the process of implementing cryptographical rule on the idea of AES. As Cryptography is that method of changing plaintext into cipher text changing keys to secure our personal knowledge. While to provide a system with security services comes at the expense of system performance.IOT devices area unit connected to internet of things. This paper deal with the implementation of AES using Internet of things and the motive is to find the elapsed time of encryption and decryption by enhancing the key generation of AES. IOT is network of physical objects, device, vehicles building. So The paper contributes the analysis of the performances of AES algorithm. AES is one of the standardized high security rule. it's enforced in varied hardware devices and varied code languages. This paper explores the implementation of AES in MATLAB. A MATLAB code is developed for plaintext encoding and cipher text decipherment.. The elapsed time will be calculated for comparing the performances of file sizes. Hence the result will show how the file size is effecting the performance of elapsed time and plotting of the graph will show the evaluation in diagrammatic forms.

Keywords: AES, Internet of things, Encryption techniques, Security, Performances analysis, Elapsed time.

I. INTRODUCTION

The cryptography consists of two main different process on the basis of keys. It is performing the transformation of public and private keys. The generation of keys will proceed to evaluate the encryption and decryption process[1]. As the earlier paper has studied about the performances of symmetric algorithm like AES, DES, RC4 with the help of evaluation the new algorithm has been generated on the basis of AES. As the internet of things is a type of network which are mainly embedded with electronics, software, network connectivity and some sensors. The internet of things permit objects to get sensed and control across your network[2].

Cryptography process: Cryptography consists of two main different process on the basis of two different keys.

Encryption: The method of converting plaintext into cipher text.

Decryption: The method of converting cipher text into plain text. These are two main important part of cryptography. The cryptography also posses two main process.

I. Private key/symmetric key: This posse's only one key.

II. Public key/asymmetric key: This key posses two different key means we will encrypt our information from IOT is augmented with some sensor as well. The main issues is securing the data and managing the IOT devices. Algorithm is generated which is mainly based on AES concepts[2].

AES is a block cipher that will calculate the number of bytes. It will currently encrypt in blocks of 16 bytes at a time. That defines AES has the block encrypt minimum of 16 bytes. AES will help to evaluate the voice encryption which will help IOT device to perform easily. As we can use remote of AC by giving the voice command which will encrypt with the help of algorithm and the same person will decrypt the algorithm back.

It is the process of utilizing software, hardware, and procedural techniques to guard applications from external dangers. Security is turning into an undeniably imperative alarm throughout development. This is because applications are regularly being accessed over networks and are helpless against a wide assortment of threats [9]. The requirements for securing applications should include privacy in multitenant atmosphere, data insurance from publicity, access control, communication protection, software security and service accessibility[3].

It also consist State which will be in the block progress.

XOR: Refers to the bitwise operator exclusive i.e. XOR it will execute in the individual bits in a byte.

Example

X1 = 1100100

X2 = 0001110

Z = 1101010 (1)

The XOR operator will be in different programming language.

Languages of Programming	XOR operator(exclusive-or)
C	^
C++	^
C#	^
Java	^
Visual basic	XOR

AES DESIGN:

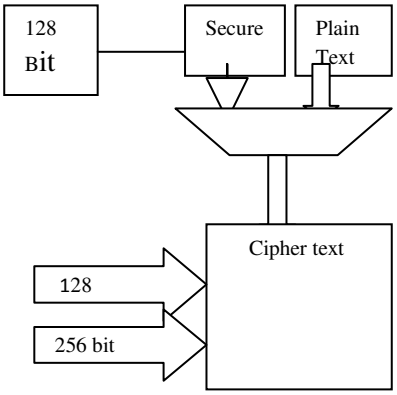

Figure 1 AES Design

ROUND:

There are two **types** of rounds

- Regular rounds(9,11,13)
- Final rounds (10,12,14)

Different rounds for different bit of keys like 192, 128, 256.

The process of rounds will consider 4 different steps:

- No. of Sub bytes
- Shifting rows
- Mixing column
- Round keys Addition

Key block round:

AES size	Key length	Block size	No of rounds
AES-128	4	4	10
AES-192	6	4	12
AEs-258	8	4	14

The performance on a two dimensional array of bytes called the state.

II. AES PROCESS:

The process will have 4 different phases in which they will take different operations based on the number of keys. The cryptography method is achieved by process plaintext and key for initial rounds[3]. The reverse method can occur within the same manner. The 4*4 matrix state is created in spherical and explicit information is introduces within the cryptography method. The 10,12,12 rounds square measure there for twelve 8,192,256 bits long ab initio a key growth method is employed to expand the idea sixteen computer memory unit key into eleven array of total forty four word. It is basically a best cryptographic process with the help of which we can encrypt our frequencies at different size. The size of the voice may vary and will result in the variation of graph. As cryptography is a science of sending secret message. The voice is encoded in some encrypted form. The process will be known as voice encryption. The person who knows how to decode this information correctly will get the original information. Whereas the csymmetric key's used for encoding in addition as for coding. On the premise of computer file. Cipher rule square measure outlined as block cipher, within which the dimensions of block is of fastened size for encoding and coding[4].

The encryption 10,12,12 rounds are there for 128,192,256 bits in length respectively. Include a key expand the basic 16 byte key into 11 arrays. Arrays are formed for the initial process and from that array key expansion will be done. Each round consist of mainly 4 different phases. Sub byte shift rows mix column and key addition. These process will be processed as according to different techniques[4].

1. 1.Substituting bytes with the help of S-box
2. To shift Row using different offset
3. Mixing data within each column of state array.
4. Addition of key with state[5].

Sub byte Phase: The sub byte transformation which operates on S-box table by using each byte. It contains 256 numbers. When we send the voice or load the voice for the encryption purpose while encrypting the signals the process will be encrypted using s-box sub-byte, all the sub byte will be loaded and the process of encryption will start. In the initialization step the creation of S-box will be done and perform its inverse S-Box, Polynomial matrices are created the creation of voices its frequency ,its size time will be done on the basis of its performances[5].

As like encryption Process

	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	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	A0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	F5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	A9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	C6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 2:Encryption process

is happened with the help of s-box the decryption will be done with the same where your encrypted voice will be decrypted by using s-box sub byte.

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

Figure 3:Inverse S-Box decryption

Shift Row:
The rows will be cyclically shift over different offsets.

Mix Column Phase:
Mixing the column will result in the final output of the system.

Generation of keys:

Here is the process of generating keys. It is nothing more than a random bit string of the right length. For a 128 bit you need 16 bytes, for a 256 bytes you need 32 bytes. If you need to generated your own AES key for encrypting data, you should use a good source. The random key will be used for generating keys and the xor operation will generate as secret keys. Symmetric-key algorithms use identical (secret) key to each apply scientific discipline protection to information8 and to get rid of or verify the protection. Keys used with symmetric-key algorithms should be illustrious by solely the entities approved to use, take away or verify the protection, and square measure normally called secret keys. A secret key's typically illustrious by multiple entities that square measure same to share or own the key, though it's not uncommon for a key to be generated, in hand and utilized by one entity (e.g., for secure storage)[6]. A secret key shall be generated.

III. MATLAB platform for AES:

It is a high level language and snug surroundings for numerical calculations mental image and programming victimisation in-built operate of this platform permits North American nation to realize result. By using the compiler of MATLAB we can generate executable code for any computer system for different environment. The applications are used with this platform over wide range like signal processing,control systems test and measurement take a view script and write the program into new script and save the file in the particular destination folder which is necessary for encryption and decryption. In the first step initialization of AES components are done like S-box and created then poly matrices and in the second step round function command is used other commands. The shift rows, matrix columns, cipher, encryption and decryption will be written.

IV. SIMULATION OF ALGORITHM IN MATLAB:

The size of plaintext of 128 bits are given as input using asymmetric key enables to perform four byte operation to get cipher text. The Four byte oriented operations involves substitution of bytes, shifting rows, mixing columns, add round key The key schedule time for this encryption and decryption are evaluated and spotted, The time will be tabulated also[8].

Experimental Result and analysis:

A block of plaintext data is given as input of AES encryption algorithm[9].

Full encryption:- This is measured exploitation the method delineated within the one spherical encoding time measurement[11].The tic toc command employed in the beginning and also the finish of the most program. The measured encoding time is eighty seven.57ms for 1st plaintext input shown within the Table one. Likewise for different eight inputs corresponding encoding times are tabulated[12].

Figure 5:Encryption Processing

Decryption time: This is measured victimization the method delineated within the one spherical cryptography time measurement. The tic toc command utilized in the

Beginning and therefore the finish of decipherment main program. The measured decipherment time is eighty eight.007ms for plaintext input shown within the Table a pair of. Likewise for different eight inputs corresponding decipherment times area unit tabulated[13].

Figure 6:Decryption processing

Results and discussion: The measured results presented higher than area unit for MATLAB implementation of AES on horsepower notebook 64bit OS, i5 processor. These results area unit compared with the results published by Sambasiva Reddy et al [2]. The MATLAB implementation is in a position execute among 88 ms, whereas Embedded Development Kit(EDK) needs two.06 s [2].The MATLAB implementation is enticing for deploying AES into numerous applications like image process, video process, etc[11].

Time of encryption and decryption for different inputs

Inputs	Value	Encryption(ms)	Decryption(ms)
Input I	00,11,22	87.588	88.009
Input II	FF,bb,ee,aa	81.900	81.250
InputIII	44,33,22,11	82.988	84.098

On the basis of data we will perform encryption processing.

OUTPUT:

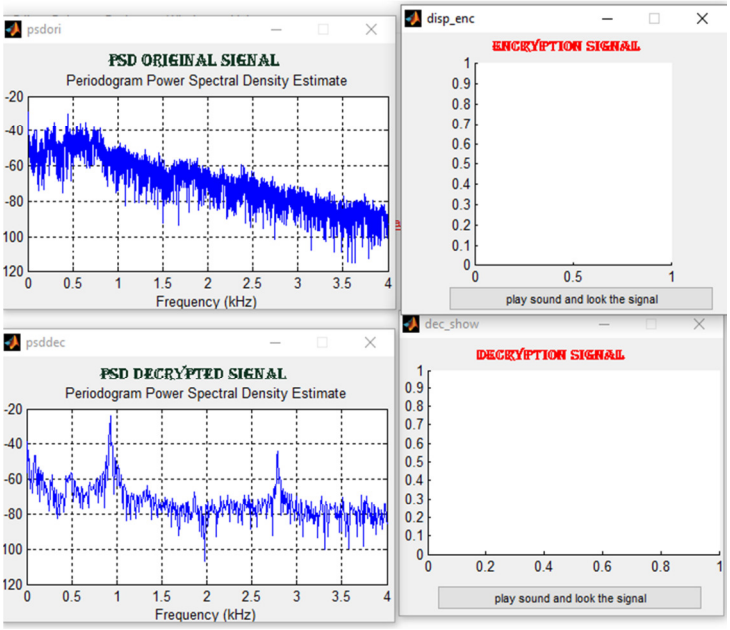

Figure 7: Encryption Algorithms with different key sizes:

. This case study is to investigate the result of adjusting the scale of cryptography key on cryptography time. file of 50.5MB is taken and totally different cipher algorithms square measure dead for various size of keys supported by them in ECB mode with PKCS#5 artifact theme. the varied key sizes mentioned in Table one square measure used throughout experimentation. Fig. four shows the results of execution for key size variation[12].

Here is that the results of cryptography and cryptography time whereas varied the scale of file. The time period is varies with the file size additionally the graph alsoshowsthescaleofinputand output.


```
Elapsed time is 0.000018 seconds.
Elapsed time is 0.000021 seconds.
Elapsed time is 0.000016 seconds.
Elapsed time is 0.000020 seconds.
Elapsed time is 0.000016 seconds.
Elapsed time is 0.000018 seconds.
Elapsed time is 0.000016 seconds.
```

Figure 7: Elapsed Timing calculation

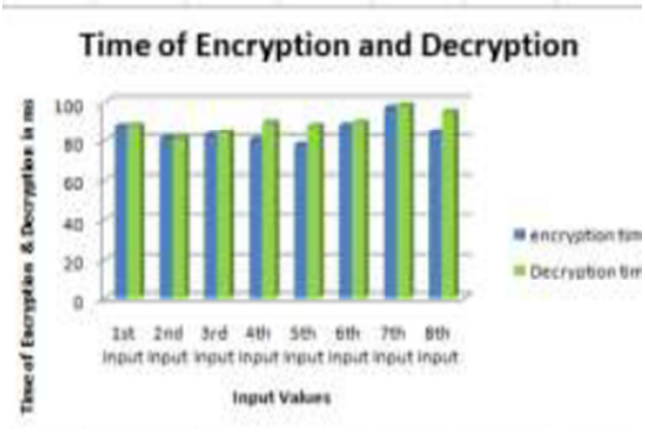

Figure 7: Timing of encryption and Decryption

These are the results of encryption generation where the difference in file size will evaluate the encryption timing[14].

V. Conclusion:

In this paper, the process of encryption and decryption is evaluating the performances of different file size. completely different files, data size, density, key size, tested however the coding time is freelance of information|. The analysis in the coding time solely depends upon the quantity of bytes of file. The variation of time period varies with completely different file size. It additionally revaluated that point varies proportional consistent with size of information.

The impact of AES coding is also studied and evaluated the impact of AES. AES coding for the system will evaluate the performance of the different file inputs. Applying AES coding will considerably effects on the system performance. The designing of the key generation has evaluated with the help of crypt tool which show how the generation of keys has been evaluate its performances.

Based on discussions during this paper and keeping in mind the importance of performance evaluation on the internet of things. It defines that enhancing the algorithm help in calculating the elapsed timing of algorithm.

REFERENCES:

[1] AL.Jeeva1, Dr.V.Palanisamy and K.Kanagaram, "Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms", *International Journal of Engineering Research and Applications (IJERA)*, Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037.

[2]Sadiya Shakil and Vineet singh "security of personal data in internet of things using cryptography algorithm,"*International journal of engineering and science computing"*

[3]Anjali Nigam and Vineet singh "A study on Data transmission Secuirty threats in cloud in "*international journal of innovative research in computer and commjncation engineering"*

[4] Nidhi Singhal and J.P.S.Raina, "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", *International Journal of Computer Trends and Technology*, Vol 2, Issue 6, July-Aug 2011, pp.177-18

[5]Allam Mousa and Ahmad Hamad, "Evaluation of the RC4 Algorithm for Data Encryption", *International Journal of Computer Science & Applications*, Vol 3,Issue 2, June 2006, pp.44-56.

[6] Aamer Nadeem, Dr M. Younus Javed, "A Performance Comparison of Data Encryption Algorithms", *First International Conference on IEEE Information and Communication Technologies (ICICT)*, Vol 1, Issue 6, 27-28 Aug. 2005, pp 84-89.

[7] Shivlal Mewada, Sharma Pradeep, Gautam S.S., "Classification of Efficient Symmetric Key Cryptography Algorithms", International Journal of Computer Science and Information Security (IJCSIS) USA, Vol. 14, No. 2, pp (105-110), Feb 2016

[8]Das Debasis, Misra Rajiv. "Programmable CellularAutomata Based Efficient Parallel *AES Encryption Algorithm*".International Journal of Network Security . Applications(IJNSA) VOL.3 No.6, November 2011.

[9]Hoang Trang and Nguyenimplementation of the algorithm" University of University HoChiMinh City Van L oi , "An efficient FPGA Advanced Encryption Standard Technology VietNam Nationa Recommendation for the Transitioning of Cryptographic Algorithms and Key Lengths, January 2011.

[10]Adam 1. Elbirt, W. Yip, B. Chetwynd, and C. Paar, "An FPGABased
Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists" IEEE Transactions On Very Large Scale Integration (Vl Si) Systems, Vol . 9, No. 4, August 2001 545

[11] Mohammed Elmogy Information Technology Dept., Faculty of Computers and Information, Mansoura University, Egypt,Internet of things. Vol. 4 No.06 Nov 2015

[12] Bolivar Torres et.al.,lntegration ofan rfid reader to a wireless sensor network and its use to identify an individual carrying rfidtags,lnternational Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol. 1, No.4, December 2010.

[13] R. Jason Weiss, Development Dimensions International. J. Philip Craiger, University ofNebraska-Omah

[14] Gartner cloud computing definition, http://www.gartner.com/itglossary/cloud-computing/

