Preventing DoS Attacks in IoT Using AES

Yasir Javed[1, 2], Adnan Shahid Khan[1], Abdul Qahar[1, 3] and Johari Abdullah[1]
[1]*FCSIT, UNIMAS, Sarawak, Malaysia*
[2]*Prince Sultan University, Riyadh, KSA.*
[3]*The University of Punjab, Lahore, Pakistan.*
yjaved@psu.edu.sa

***Abstract*—The Internet of Things (IoT) is significant in today's development of mobile networks enabling to obtain information from the environment, devices, and appliances. A number of applications have been implemented in various kinds of technologies. IoT has high exposure to security attacks and threats. There are several requirements in terms of security. Confidentiality is one of the major concerns in the wireless network. Integrity and availability are key issues along with the confidentiality. This research focuses on identifying the attacks that can occur in IoT. Packet filtering and patches method were used to secure the network and mitigate mentioned attacks but these techniques are not capable of achieving security in IoT. This paper uses Advanced Encryption Standard (AES) to address these mentioned security issues. Official AES version uses the standard for secret key encryption. However, several problems and attacks still occur with the implementation of this original AES. We modified AES by adding white box and the doubling of the AES encryption. We also replaced the Substitute-Byte (S-Box) in the conventional AES with the white box. The significance of a white box is where the whole AES cipher decomposed into round functions. While doubling the process of AES gives difficulty to the attacker or malware to interrupt the network or system. From the algorithms, our proposed solutions can control DoS attack on IoT and any other miniature devices.**

***Index Terms*—DoS Attack; AES; IoT Security; Confidentiality; White Box.**

I. INTRODUCTION

The inventions of smart devices and mobile devices are growing very rapidly as the development of mobile computing is also increasing with all of them including Internet of Things (IoT) as their integral part. IoT are objects that are uniquely identifiable and have Internet-like structure virtual representation [1]. The growth of IoT nowadays is enormous. Modern technologies such as Radio-Frequency Identification (RFID), sensor networks, short-range wireless communications, and real-time localization are now becoming extremely usual, which apply IoT into commercial use. There are wide range of networks such as Wireless Sensor Network (WSN), Vehicular Ad-Hoc Network (VANET), Radio-Frequency Identification (RFID), Smartphone, and others, are included in constructing the IoT [2]. There are billions of IoT devices connected today and are expected to increase in coming years. Because of wide range of applications, elements in IoT interact via broadcasting messages, which create the messages' dissemination efficient. This make IoT network prone to attacks, where attacker to interrupt the networks. It will be easier for attacker to intercept, fabricate or even steal the data in the networks that might be the high-secrecy or private confidential information. All these suggested solutions are applicable in the real time applications. People's requirements for improved living condition are constantly rising because of the development of economy and the rise of information-based society. Building Smart Home based on the advancement information technology is becoming more important. It is essential to process and use the immense and decentralized information. Smart home is the basis component of Intelligent Residential District [3]. The user can correspond with the latest security dynamics of the whole family if security devices, such as infrared detector, smoke sensor, etc. can be accessed to the IoT network. To access to the network of IoT and community hospital, user need to have household medical devices like sphygmomanometer so doctors can correspond with the patients' health condition timely and make treatment. Family business center can complete a series of tasks, such as shopping and payment so people can stay indoors to manage their daily life [4]. Thus, the security requirements are the major concern regarding these problems. One of the key problems is the leak of personal information that shows the violation of confidentiality. The integrity issue come through when there is a stealing of data and identity. Attacks on integrity can disable the sensing and control the information. Availability is another great target for the attacks. This research focuses on Denial of Services (DoS) attack that is high possibility to occur when it comes to availability context. DoS attack occurs when the system or service that is required cannot be accessed. Thus, securing broadcast communication protocol is conducted into research. This research proposes several improvement in AES encryption structure. White box as stated, it decomposes the whole AES cipher into round functions.

Section II presents the related works, about known AES mechanism and their modification, Section III presents a system model Section IV presents the proposed solution. Section V presents the mathematical analysis of proposed solution. Section VI presents the conclusion.

II. RELATED WORKS

AES replaces the Data Encryption Standard (DES) in 2001 [4-6]. AES contains ten iterations of four key operations, which are the SubBytes, ShiftRows, MixColumns and AddRoundKey [7]. Security and confidentiality have always been the major concern of cloud consumers since the beginning. Such concerns are derived from several types of attacks on several systems that have occurred since these cloud-based services are implemented. Brute force attack, also known as Dictionary attack or Hybrid Brute-force attack is one of the incorporate attacks. According to Whitney [8], brute-force attack is an attack that uses "Trial and Error" method by guessing users' passwords. This method initially

initiated by gathering the fundamental information about the user such as user's nickname, pet name, birthday month or year and vehicle name. Attackers usually launch this method by combining random and guessable passwords such as '1234' or 'qwerty'. In 2013, October 3 to be exact, Adobe has confirmed that it had been a victim of an attack that affected 38 million of active users—which mostly used guessable and random words as their passwords [9]. This brute force attack enables attackers to guess users' passwords using a key derivation function, known as exhaustive key search. This attack is a cryptanalytic attack that used to decrypt or crack any encrypted data.

Jose [10] has proposed a technique called "SecCloud Protocol Implementation" which encrypted protocol data and sent it to the cloud servers. This technique initially used RSA algorithm for encryption, but since it suffered from brute force attack, another AES algorithm has been introduced to solve this problem. However, brute force attacks still exist since the author did not focus on the S-box model. Meanwhile, Junjie and Feng [11] proposed a solution by using an expansion key on AES algorithm to improve the security of the key and maintaining the algorithm efficiency at the same time. This solution proposed does increase the security, but it does not increase the key length, which might be a problem since brute force attacks target on key length.

Al-Haj et.al [12] have chosen as the AES in 2001 after an open process because of its efficiency, security, implement ability, flexibility, and performance. There are many applications using AES since it gives many benefits such as remote diagnosis contribute by telemedicine applications access to centralized medical remote-distance learning and medical archives. They suggested improvised method, which they provide the encryption keys and initialization vectors externally so that it can overcome the overhead.

White box as stated, it decomposes the whole AES cipher into round functions. The output of previous round is the offset of the input of encoding in the ith round. All the encodings is produced through both linear and non-linear mapping. Next, the shiftrows transformation that we suggested is the simple permutation process, which is circular byte shift that can be guaranteed. Mix columns also applicable where the four bytes in each column of a state is combine with an invertible linear transformation. We proposed the AES add round key algorithm adapted from Rijndael algorithm[13]. In this algorithm, the 128-bit independent key for every round is derived from the original 128-bit encryption key. Our research proposed a doubling process of AES with two different keys. It will ensure the attacker not to disrupt the network or system because it is strengthen by the double encryption of AES. AES uses byte wise substitution, byte swapping and the XOR operation for encryption process. The mathematical analysis for this operation is when 128-bit plaintext block are arranged into 4x4 columns. It called 'states' and to generate 128 bits of cipher text it will undergo 10 rounds. At the same time, the key expansions also occur. The 128-bit keys will produce other 128-bit keys for 10 rounds. Ten (10) matrices are made up from the arrangement of keys in 4x4 matrices.

III. System Model

Figure 1 represents a system design for our proposed model where a user would like to upload the data into cloud. For This a Cloud User will use our extended AES Encryption standard to store the data. Where the Data owner if want to see the data has to decrypt the cipher using his known key. Thus, Cloud user will be able to send the data securely over the cloud and data owner while using the secret key can see it.

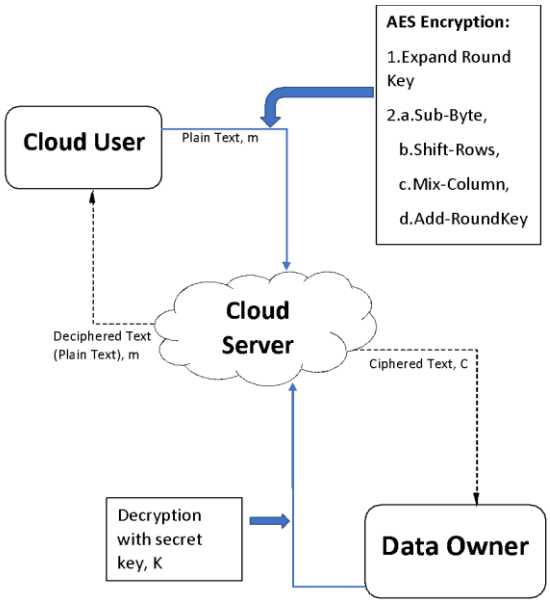

Figure 1: The implementation of AES on IoT (Cloud Service)

Figure 2 represent a DOS attack, where attacker has stopped the services to Data owner.

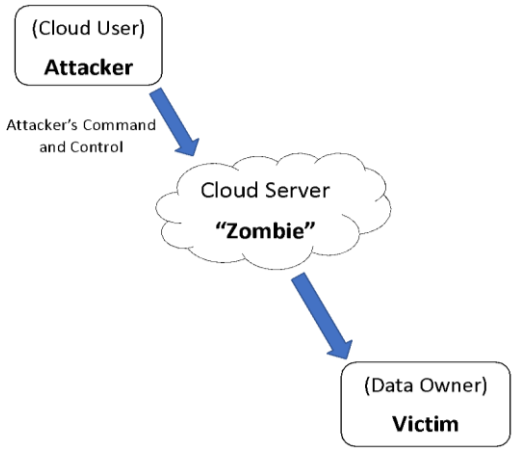

Figure 2: The DoS attack on IoT (Cloud Service)

Internet has become a mission- critical component in modern business. Having said that, cybersecurity has become indispensable element in the information system. However, threats and attacks are inevitable in the cyber world due to lack of security [5]. The IoT is not an exception to this problem. One of the problems arose is the unwanted release of personal information. It is the violation of data confidentiality [14]. For example, a data leak in the smart medical center monitoring system will lead to an inadvertent release of sensitive medical data. Therefore, loss of confidentiality in passwords and important keys will cause unwanted system threats. Furthermore, attacks on integrity can distort the sensing and control information [15]. For instance, the house controller confused by unauthenticated system status alerts will predicted a situation mistakenly which allowed an illicit entry. Availability becomes the greatest target for the attacks. Many Internet-enabled devices often configured with default or weak password. For instance,

in-car Wi-Fi has the same security vulnerabilities as traditional Wi-Fi hotspots. However, in-car devices and data will be at risk without the firewalls present in conjunction with Wi-Fi installation. Hence, as more and more products are developed with the capacity to be networked, wirelessly networked IoT devices with a low operational duty cycle will flood the network and this can lead to a denial of service to legitimate users.

IV. PROPOSED SOLUTION

A. Reminiscing the Old Solution

As stated in the problem statement, one of the common services that facing DoS is the network device level. Previously, the two common ways in preventing this matter were patches method and packet filtering. For instance, to hinder the attacks, it is better for a network to reject broadcast ping requests to reach the network from outside, or to configure a firewall that rejects all arriving echo request packets. Suppose that the Internet Service Provider (ISP) in Figure 1 owns the router that give the end network internet access and the ISP knows the legal address size of packets trying to reach through this router. If a packet is trying to reach the ISP and act to be from an address that is outside of this legal address space, thus it is clearly depicted. The deception attempt can be logged and the packet can be filtered out.

B. Newly Proposed AES Encryption

However, filtering packets and patches method were not robust enough to secure the network security. Here, we have indicated a couple of new algorithm to modify the existing AES, which are the doubling of the AES encryption, and the white box, which replaces the Substitute Bytes (S-Box). Below are the explanation for the method used in AES encryption that can prevent the attack techniques of DoS such as Attack Tools, Application-layer Floods, Degradation-Of-Services and Denial-Of-Services from occurring [15]. Therefore, the most suitable encryption protocols for device to server communications is AES.

1) Independent Key (Round Key)

The key will be arranged in the form of 4x4 bytes matrix then it will be expanded into a schedule 44 words. The independent key will be added into the input block of plaintext to be ciphered once it is expanded [16].

2) Input Block

The first word from the key fills the first column of the matrix. The expanded independent key is arranged into a schedule of 44 words. Each round during the AES encryption will contain 4 words from the schedule. Thus, the input block contains a plaintext from the client side and expanded independent key.

3) Input State Array

Before the round-based process for encryption commence, the input state array is XOR with the first four words from the schedule (44 words of expanded independent key).

C. Proposed AES Encryption Structure

1) White box cryptography (WBC)

Even though the implementation of white box will expose an encryption algorithm to the external, white box is defended by encoding, mixed bijections and external encoding. During the encoding, a bijection of two keys are injected into the lookup tables from the Sub-Bytes process. Apart from that, mixed bijections will add confusion by concatenate input and output from the encoding [16]. In addition, external encoding will double the number of lookup tables. Although white box provides full visibility of internal algorithm, it is just to consider the worst-case attack model [3, 6].

2) Sub-Bytes/S-box

SubBytes dominates the AES performance. There are two implementations to utilize the Sbox in SubBytes. The first approach was implementing the composite-field computation-based Sbox on FPGAs. Then another was the LUT (LookUp Table). The former involves mapping and inverse mapping between the GF (28) field and the GF (24) field. While the latter one applies the formula, $\mathbf{Lsb = 8 - K + 1}$, K is the number of inputs in LUT [4].

3) Shift Rows

This Shift Rows transformation is a simple permutation (circular byte shift) process that will guarantee. For example, in the first row, there is no byte to shift whereas at the second row, there is a 1-byte circular left shift and followed by the third row, a 2-byte circular left shift. Finally, the last row by three bytes to the left. The shifts of row will help to complicate the cryptanalysis that intrudes a cloud service.

The input block is in the form of column-wise. The first four bytes of the input block will fill up the first column of the state array, followed by the next four bytes of the second column, and so on. In the end, the byte order of the input block is scrambled up due to the rows shifted in the indicated manner.

4) Mix Columns

In this step, combine the four bytes in each column of the state with an invertible linear transformation. During the Mix Column operation, four bytes are taken as input and then outputs another four bytes, where each input byte influences the four outputs. Along with the Shift Rows, another step in the AES encryption, which is the Mix Columns, provide diffusion in the cipher. A fast and low complexity architecture for the Mix Column in AES operation is proposed. It is recommended to contain a short critical path, small gate count and versatility (encrypt and decrypt) [4].

5) Add Round Key

A round key will be derived from the original 128-bit encryption key in every round. The XOR of the round key (independent key) with the state array is a part of one of the four steps available in both AES encryption and decryption. The AES AddRoundKey algorithm is applied to derive the 128-bit independent key for every round from the original 128-bit encryption key. In addition, the logic behind the independent key expansion algorithm is to guarantee that if one bit of the encryption key is altered, the independent keys for several rounds will be affected as well. Having said that, the same manner goes to the 128-bit input block is arranged in the form of state array, the algorithm organize the first 16 bytes of the encryption key in the form of 4x4 array of bytes.

6) Double the process of AES encryption in IoT with two different keys.

If the hacker tend to send a malware that can interrupt, inhibit the normal flow of data into and out of the system or disrupt the IoT such as Smart Home System, the AES will double encrypt by using two different keys, the malware will unable to break the algorithm because it has been strengthen by the double encryption process of AES [8]. Hence, the system will be unable to disrupt by the hacker thus the user able to access to the system as usual [6].

The data encryption and decryption above is for AES-128 bits. In order to make the data even more secure, we apply the 192 bits or 256 bits. Furthermore, in the near future, we can produce the IoT board, which is a black box that can receive the plain text as input and gives encoded output for various IoT applications [4]. Having said that, even a common computer user can secure data.

V. AES MATHEMATICAL ANALYSIS

A. White-Box Implementation

1) Encoding

The aim is to make the extraction of the key from the encryption code harder due to a new complicated lookup table. The bijection of key g and f.

$$T^1 = g_0\ T_0\ f^{-1}$$

2) Mixed bijection

A concatenation of input and output from the previous encoding.

3) External Encoding

The double of lookup tables in the 1st to the 9th iteration after the mixed bijection will produce:

228 of 8- bit to 32-bit lookup tables 1024 bytes each.
1728 of 8-bit to 4-bit lookup tables which is 128 bytes each.
16 of 8-bit to 8-bit lookup tables which is 256 bytes each.

Thus, the attacker will find it tedious to search through the large storage for cryptanalysis.

Operations in AES are performed using bytes. There are $2^8 = 256$ number of bytes possible. Specific bytes are represented by elements in the finite field,

$$F = \frac{Z[x]}{p(x)}$$

where $p(x) = x^8 + x^4 + x^3 + x + 1$ (according to original Rijndael algorithm). Other choices for p(x) can be used also.

B. S-box

S-box is used to transform a given element in $F = \frac{Z_2[x]}{p(x)}$ into another unique element in F using the AES S-box.

For e.g. $p(x) = x^4 + x^2 + x$
Binary presentation of $p(x) = 00010110$
Split it into two sides.

LHS
Binary presentation= 0010
Binary expression= $0.2^3 + 0.2^2 + 1.2^1 + 0.2^0$
Binary expression = 1

RHS
Binary presentation= 0110
Binary expression= $0.2^3 + 1.2^2 + 1.2^1 + 0.2^0$
Binary expression = 6

Entry 1 will be used as row and 6 will be used as column. Referring to the AES S-box, we will gain 71, which as a byte can be expressed as 010000111, and as polynomial can be represented by. $p(x) = x^6 + x^2 + x + 1$.

Thus, for the input $p(x) = x^4 + x^2 + x$will produce output $p(x) = x^6 + x^2 + x + 1$.

C. SubByte

The input encoding of the i th round is offset by the output of previous round and the encoding is composed of non-linear mapping and linear mapping with the formula,

F = g. E. f
= Q. B. M. S. A. P
= QBMSAP

where: f = input encoding,
A = block diagonal linear mapping
P = nonlinear mapping
M = invertible linear mapping
S = the concatenation of S-box on m bits
E = 4F
Q = non-linear mapping
B = block diagonal linear mapping

Let x=($x_{1,\dots,}x_4$), S=($S_{1,\dots,}S_4$), AP=($P_{1,\dots,}P_4$),and M=[$M_{1|\dots|}M_4$], where x_i's are 8-bit values, P_i's are nonlinear bijections on 8 bits and M_i is the ith vertical strip of size 32 × 8. For $1 \le i \le 4$,

F(x) = QBMSAP(x)
= ($\Sigma M_i 4_i$=11$S_i P_i$ (x_i))
= Q ∘ (ΣQ−1 ∘(x_i))

The nonlinear part Q can be removed up to an affine transformation in ((n/mQ)23mQ) when Q = (Q1,..,Qn/Qm) and each Qi is a nonlinear bijection on mQ bits. After the nonlinear P and Q are removed, the equation becomes F = B∘ S∘ A. The specialized affine equivalence algorithm (SAEA) with (n322n) is applied into the equation. *A* and *B* in O ((n/m) mA323m) can be found, where mA is the smallest integer p such that A is a block diagonal matrix with p×p matrix blocks. Matrix block will be convert using S-box to produce a new matrix B_i.

$$B_i = [b_{i:0,0}\ b_{i:0,1}\ b_{i:1,0}\ b_{i:1,1}\ b_{i:0,2}\ b_{i:0,3}\ b_{i:1,2}\ b_{i:1,3}\ \ b_{i:2,0}\ b_{i:2,1}\ b_{i:3,0}\ b_{i:3,1}\ b_{i:2,2}\ b_{i:2,3}\ b_{i:3,2}\ b_{i:3,3}\ ]$$

D. ShiftRow

Let state be S_i where i=1, 2, 3,…, r, round=number of rounds

$$S_i = \begin{bmatrix} S_{i:1,1}\ S_{i:1,2}\ S_{i:2,1}\ S_{i:2,2}\ \ S_{i:1,3}\ S_{i:1,4}\ S_{i:2,3}\ S_{i:2,4}\ \ S_{i:3,1}\ S_{i:3,2} \\ S_{i:4,1}\ S_{i:4,2}\ \ S_{i:3,3}\ S_{i:3,4}\ S_{i:4,3}\ S_{i:4,4} \end{bmatrix}$$

After shift row,

$$S_i = [S_{i:1,1}\ S_{i:1,2}\ S_{i:2,2}\ S_{i:2,3}\ \ S_{i:1,3}\ S_{i:1,4}\ S_{i:2,4}\ S_{i:2,1}\ \ S_{i:3,3}\ S_{i:3,4} \\ S_{i:4,4}\ S_{i:4,1}\ \ S_{i:3,1}\ S_{i:3,2}\ S_{i:4,2}\ S_{i:4,3}\ ]$$

E. MixColumn

This operating involve the modular multiplication of 2 four-term polynomials whose coefficients are element of $GF(2^8)$. All the columns in state are treated as four terms polynomial

$b(x) = b_3x^3 + b_2x^2 + b_1x + b_0$ and
$a(x) = a_3x^3 + a_2x^2 + a_1x + a_0$.

Polynomial multiplication

$$a(x) \cdot b(x) = c(x) = (a_3x^3 + a_2x^2 + a_1x + a_0) \cdot (b_3x^3 + b_2x^2 + b, x + b_0) = c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x^1 + c_0$$

where:

$c_0 = a_0b_0$
$c_1 = a_ib_0 \oplus a_0b_1$
$c_2 = a_2b_0 \oplus a_1b_1 \oplus a_0b_2$
$c_3 = a_3b_0 \oplus a_2b_1 \oplus a_1b_2 \oplus a_0b_3$
$c_4 = a_3b_1 \oplus a_2b_2 \oplus a_1b_3$
$c_5 = a_3b_2 \oplus a_2b_3$
$c_6 = a_3b_3$

Modular reduction

Since the outcome of c(x) has 7-term polynomial, it has to be reduced to 4 term, as it need to be in 4-byte word.

$$a(x) \otimes b(x) = c(x) mod(x^4 + 1)$$
$$= (c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_0) mod(x^4 + 1)$$
$$= c_6x^{6mod(4)} + c_5x^{5mod(4)} + c_4x^{4mod(4)} + c_3x^{3mod(4)} + c_2x^{2mod(4)} + c_1x^{2mod(4)} + c_0x^{0mod(4)} = c_6x^2 + c_5x + c_4 + c_3x^3 + c_2x^2 + c_1x + c_0$$
$$= c_3x^3 + (c_2 \oplus c_6)x^2 + (c_1 \oplus c_5)x + c_0 \oplus c_4$$
$$= c_3x^3 + (c_2 \oplus c_6)x^2 + (c_1 \oplus c_5)x + c_0 \oplus c_4$$
$$= d_3x^3 + d_2x^2 + d_1x + d_0$$

where:

$d_0 = c_0 \oplus c_4$
$d_1 = c_1 \oplus c_5$
$d_2 = c_2 \oplus c_6$
$d_3 = c_3$

Matrix representation

Using polynomial multiplication,

$d_0 = a_0b_0 \oplus a_3b_1 \oplus a_2b_2 \oplus a_1b_3$
$d_1 = a_1b_0 \oplus a_0b_1 \oplus a_3b_2 \oplus a_2b_3$
$d_2 = a_2b_0 \oplus a_1b_1 \oplus a_0b_2 \oplus a_3b_3$
$d_3 = a_3b_0 \oplus a_2b_1 \oplus a_1b_2 \oplus a_0b_3$

Replace coefficients of a(x) with the constants [3 1 1 2], we will get:

$d_0 = 2b_0 \oplus 3b_1 \oplus 1b_2 \oplus 1b_3$
$d_1 = 1b_0 \oplus 2b_1 \oplus 3b_2 \oplus 1b_3$
$d_2 = 1b_0 \oplus 1b_1 \oplus 2b_2 \oplus 3b_3$
$d_3 = 3b_0 \oplus 1b_1 \oplus 1b_2 \oplus 2b_3$ Or,

$$[d_0\ d_1\ d_2\ d_3\ ] = [2\ 3\ 1\ 2\ \ 1\ 1\ 3\ 1\ \ 1\ 1\ 3\ 1\ \ 2\ 3\ 1\ 2\ ][b_0\ b_1\ \ b_2\ b_3\ ]$$

F. AddRoundKey

Each Round Key consist of Nb words from the key schedule are each added into the column of the state, such that $[S'_{0,c}, S'_{1,c}, S'_{2,c}, S'_{3,c}]$ $[S_{0,c}, S_{1,c}, S_{2,c}, S_{3,c}]$ • $[W_{round\ FNB}\ ]$ for 0 • c < Nb.

The key matrix K_i where i=1,2,…,r-1 will be added to matrix D_i resulted from MixColumn. This will produce A_i where i=1,2,…,r-1.

$$A_i = K_i + D_i$$

For the first round i=1,

For i=r, formulae

$$A_r = K_r + C_r$$

where C_r was output of ShiftRow,

A_r=cipher text

is used because MixColumn transformation is not repeated in final round. A_r . This proves that our proposed method is more secure in terms of avoiding the attacks especially the DoS attack. It can be used in IoT setting anywhere, as it will ensure that Man-in-the-Middle attack will not occur. In future, we plan to test our algorithm on IoT devices and check its security and execution time to benchmark it with other security algorithm.

VI. CONCLUSION

This paper presented novel AES implementation with a simple and integrated countermeasure against Denial of Services Attack (DoS) in IoT. IoT can be divided into smart grid, smart car, smart campus, smart house, wearables and industrial internet. The security involves the measures and controls that ensure confidentiality, integrity and availability of the information processed. However, there are some of the attack techniques of DoS such as Attack Tools, Application-layer Floods, Degradation-Of-Services and Denial-Of-Services. Rijndael algorithm incorporates four transformations namely SubBytes, ShiftRows, MixColumns and lastly is AddRoundKey in each round step and it is a uniform and parallel composition. AES has a strong symmetric key cryptographic algorithm, which uses table of lookups. To carry out the encryption and decryption, AES need a minimum of 128 bits or 192 bits with recommendation of 256 bits cryptographic keys. The algorithms is composed of three layers, which are linear diffusion, non-linear diffusion and key mixing. The new design and idea allows the construction of the actual cores with speed characteristics and efficient area. Protecting against the threats and attacks in the cyber world still need to be investigate and excavation however it is still a challenge and it is also costly. Development of the efficient countermeasures for the prevention of the side-channel attacks in IoT is one of the open issue in scientific world and it should be further investigated optimized in the future research by human. The proposed algorithm will be compared against present security algorithms for security effectiveness and their effect on memory as well as computational usage.

ACKNOWLEDGEMENT

The work is fully funded by Research and Innovation Management Center (RIMC) under the grant number F08/SpSG/1403/16/4.

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645-1660, 2013.

[2] B. Li, J. Yub, "Research and application on the smart home based on component technologies and Internet of Things," *Advanced in Control Engineering and Information Science*, vol. 15, pp. 2087 – 2092, 2011. Retrieved from http://www.sciencedirect.com.

[3] M. A. Zaveri, S. K. Pandey, and J. Kumar, "Collaborative service oriented smart grid using the Internet of Things," In *Communication and Signal Processing (ICCSP), 2016 International Conference on*, pp. 1716-1722, Apr. 2016. IEEE.

[4] S. Pawel, "FPGA Trojans through detecting and weakening of cryptographic primitives," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 8, pp. 1236-1249, 2015.

[5] A. A. Panmu, K. S. Chong, W. G. Ho, and B. H. Gwee, "Interceptive Side Channel Attack on AES-128 Wireless Communications for IoT Applications," *Asia Pacific Conference on Circuits and System 2016*, pp. 650-653, 2016.

[6] G. Singh, "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security," *International Journal of Computer Applications*, vol. 67, no. 19, 2013.

[7] M. M. Wong, M. L. D. Wong, A. K. Nandi, et al., "Composite field GF(((22)2)2) Advanced Encryption Standard (AES) S-box with algebraic normal form representation in the subfield inversion," *IET Circuits Devices Syst.*, vol. 5, no. 6, pp. 471–476, May 2011.

[8] L. Whitney, Adobe hack attack affected 38 million accounts, 2013. Retrieved from CNET: https://www.cnet.com/news/adobe-hack-attack-affected-38-million-accounts/.

[9] C. Paar, J. Pelzl, and B. Preneel, *Understanding Cryptography: A Textbook for Students and Practitioners*, 2010. Springer.

[10] A. Jose, "SecCloud Protocol Implementation Using AES Algorithm for Security and Privacy in Cloud Computing," *2014 International Journal for Research in Applied Science and Engineering Technology*, vol. 2, no. 2, pp. 1-8, 2014.

[11] J. Yan, F. Chen, "An Improved AES Key Expansion Algorithm," *International Conference on Electrical, Mechanical and Industrial Engineering*, 2016.

[12] A. Al-Haj, G. Abandah, and N. Hussein, "Crypto-based algorithms for secured medical image transmission," *IET Information Security*, vol. 9, no. 6, pp. 365-373, 2015.

[13] S. Srinivas, "FPGA Based Hardware Implementation of AES Rijndael Algorithm for Encryion and Decryption," *International Conference on Electrical, Electronics, and Optimization Techniques*, pp 1769-1776, 2016.

[14] N. Ruan and Y. Hori, "DoS atack-tolerant TESLA-based broadcast authentication protocol in Internet of Things," *International Conference on Selected Topics in Mobile and Wireless Networking*, pp 60-65, 2012.

[15] Y. Yuan, H. Yuan, L. Guo, H. Yang, and S. Sun, "Resilient Control of Networked Control System Under DoS Attacks: A Unified Game Approach," *IEEE Transactions On Industrial Informatics*, vol. 12, no. 5, pp. 1786-1794, 2016.

[16] N. Mathu and R. Bansode, "AES Based Text Encryption Using 12 Rounds With Dynamic Key Selection," *7th International Conference on Communication, Computing and Virtualization 2016*, pp.1036-1043, 2016.

[17] Q. Liu, Z. Xu, and Y. Yuan, "High throughput and secure advanced encryption standard on field programmable gate array with fine pipelining and enhanced key expansion," *IET Computers & Digital Techniques*, vol. 9, no. 3, pp. 175-184, 2015.