ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

# An Encryption-Decryption Scheme towards Higher Level Cyber Security of Authenticated Data

[1]T.Archana, [2]K.Aswini , [3]P.Susanna, [4]Mrs.Sivagami B.E ,M.E,M.B.A,(Ph.d)

Final Year, Department of ECE, Sriram Engineering College, Perumalpattu, Chennai, TamilNadu, India, [1,2,3]

Assistant Professor, Department of ECE, Sriram Engineering College, Perumalpattu, Chennai, TamilNadu, India[4]

**ABSTRACT:** Internet of things ,internetworking of smart devices, embedded with sensors, software, electronics and net-work connectivity that enables to communicate with each other to exchange and collect data through an uncertain wireless medium. Recently IoT devices are dominating the world by providing it's versatile functionality and real-time data communication. Apart from versatile functionality of IoT devices, they are very low-battery powered, small and sophisticated, and experience lots of challenges due to unsafe communication medium. Despite the fact of many challenges, the energy issue is now becoming the prime concern. Optimization of algorithms in terms of energy consumption has not been explored specifically, rather most of the algorithms focus on hardware area to minimize it extensively and to maximize it on security issue as possible. But due to recent emerge of IoT devices, the main concern is shifting to moderate security and less energy consumption rate. We present MAES, a lightweight version of Advanced Encryption Standard (AES) which meets the demand. A new 1-dimensional Substitution Box is proposed by formulating a novel equation for constructing a square matrix in affine transformation phase of MAES. Efficiency rate of MAES is around 18.35% in terms of packet transmission which indicates MAES consumes less energy than AES and it is applicable for Resource Constraint Environments.

## I. INTRODUCTION

Internet of Things (IoT) is the next revolution of the internet which brings profound impact on our everyday lives. IoT is the extension of the Internet to connect just about everything on the planet. This includes real and physical objects ranging from household accessories to industrial engineering.

As such these “things” that are connected to the Internet will be able to take actions or make decisions based on the information they gather from the Internet with or without human interaction. In addition, they also update the Internet with real-time information with the help of various sensors. IoT works with resource-constraint components such as sensor nodes, RFID tags etc. These components have low computation capability, limited memory capacity and energy resources, and susceptibility to physical capture. Also, they communicate through the wireless communication channel which is not secured and transmit real-time information through the treacherous wireless medium. In certain applications, confidentiality, authentication, data freshness, and data integrity might be extremely important. Therefore, encryption of data is becoming a major concern. But due to resource-constraint nature of the components, short-term security can meet the demand. By the term resource-constraint means low battery power, less computational speed etc.

Encrypting data using standardized cryptographic algorithms may consume more energy which drastically reduces 0the lifetime of the components. Two main approaches are followed to design and implement security primitives which are fitted with extremely constraint devices.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Firstly, designing new lightweight cryptosystem. For instance, are some recently proposed lightweight cryptographic algorithms. Secondly, modifying the existing standard cryptosystem in a lightweight fashion. Possible examples of the second approach are modification of the Advanced Encryption Standard Algorithm.

## II. PROPOSED SYSTEM

With respect to the security aspect and implementation complexity, AES is considered as one of the strongest and efficient algorithms. Despite that like other symmetric encryption algorithms, the secret key distribution is still considered as a critical issue. Again to encrypt or decrypt a single block (128-bit) of data, an essential amount of computational processing has to be done which consumes enormous battery power. As components of IoT have resource-constraint characteristics, consuming immense power may cause expiration of such components. Analyzing related work, we come to know that Substitution Layer is the most energy consuming portion of AES in the round based design. Considering energy consumption of resource-constrained components of IoT, we are proposing MAES, a lightweight version of AES where we reduce the computation of Substitution Box (S-Box) of AES.
The contribution of the proposed work can be summarized as follow:

We propose 1-dimensional Substitution Box (S-Box) which is constructed by formulating a novel equation for constructing a square matrix in affine transformation phase of MAES.

We implement both original AES and MAES algorithms on TinyOS 2.1.2 platform in TelosB sensor mote using MTS400 as sensor board along with TI MSP430 microcontroller and CC2420 radio chip.

After analyzing the result of our experiment we conclude that MAES is well efficient than AES in terms of number of packet transmission and latency.

## III. RELATED WORKS

In recent years, many research works have been undergone and significant achievements have been found by many renowned researchers with respect to Resource Constraint Environments (RCEs). However, most of them have targeted low area and low power as their concerned aspect and are hardware oriented. To illustrate implementation choice of the block cipher, Bogdanov have investigated how the variation in the architecture of S-Box/MixCloumn, frequency of the clock cycle and unrolling the design can affect the energy consumption. Their model is validated by estimating the energy consumed by several lightweight algorithms. With the help of figures, the proposed model is compared with respect to the different degree of unrolling. Moreover, they have proved that total energy consumption in a circuit during an encryption operation has roughly a quadratic relation with the degree of unrolling and the most energy consuming part is Substitution Box (S-Box) in 2-round unrolled design.

Feldhofer et. al. and Moradi et. al. have proposed an implementation of AES and its basic transformations (such as S-Box) targeting low area and low power. All the implementations are mostly hardware oriented. Design is based on an 8-bit datapath and approximately occupies 3400 Gate Equivalents (GE) and design features a mixed datapath and requires 2400 GE respectively.

Felicisimo et. al. have proposed two Substitution Boxes, where the first S-Box is the Rijndael S-Box and the second S-Box, replacing the MixColumns operation of the original AES, is constructed through an XOR operation and affine transformation. Based on simulation testing, it is found out that the modified AES algorithm using multiple S-Boxes has better speed performance compared to the original cipher. Kawle et. al.have proposed a modified AES using state-of-art techniques to reduce computational overhead of the original AES algorithm by encrypting large size data, for instance, multimedia data.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

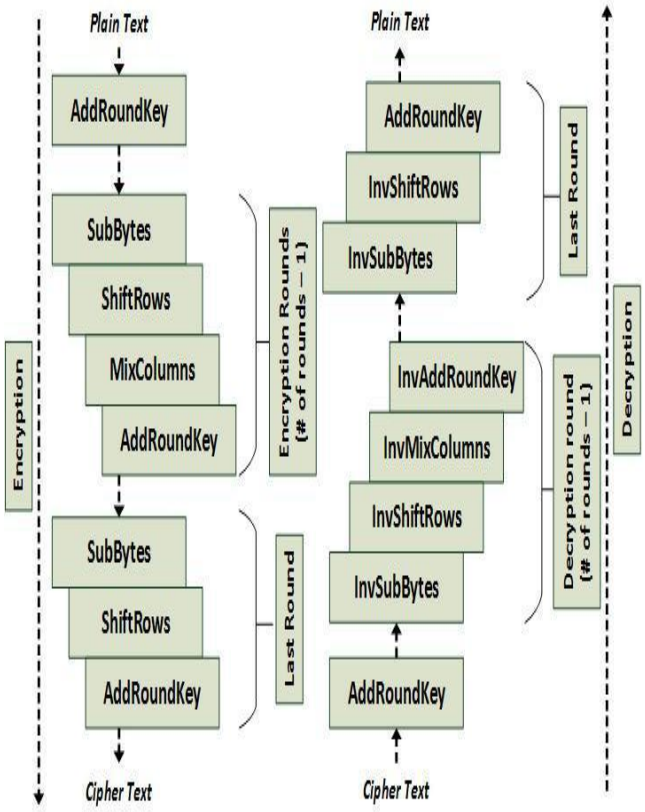
Vol. 8, Issue 3, March 2019

## IV. PRELIMINARIES

The Advanced Encryption Standard (AES) , a symmetric key block which is published by the National Institute of Standards and Technology(NIST) in December 2001. It is a non-Feistel block cipher that encrypts and decrypts a fixed data block of 128-bits. There are three

different key lengths. The encryption/decryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

AES performs several rounds where each round is made of several stages. A data block is transformed from one stage to another. Before and after each stage, the data block is referred to as a state. Each round, except the last, performs four trans-formations which are invertible. The last round implements the rest three transformations except the MixColumns stage. Figure 1 shows the AES cipher structure. Each round has four stages to achieve the MAES performance.




**FOUR STAGES:**

1. **Substitute Bytes:** The first transformation, SubBytes, is used at the encryption site. It is a non-linear byte substitution that operates independently on each byte of the state using a substitution table (S-Box). All the 16 bytes of the state are substituted by the corresponding values which are found from the lookup table. In decryption, InvSubBytes is used. Bytes of a state are substituted from InvSubBytes table. Figure shows the SubBytes operation.

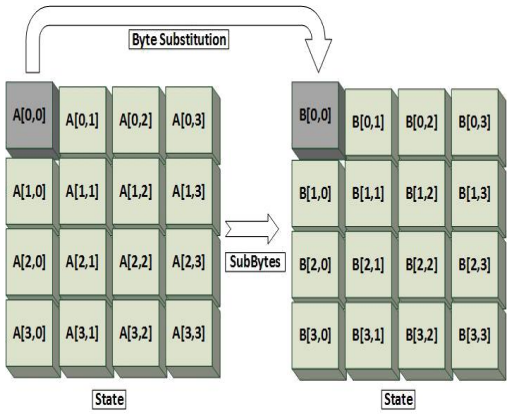
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019




**2. Shift Rows:** In the encryption, the state bytes are shifted left in each row. It is called ShiftRows operation. The number of the shifts depends on the row number (0, 1, 2 or 3) of the state matrix. Row 0 bytes are not shifted and row 1, 2, 3 are shifted to 1, 2, 3 bytes left accordingly. Figure shows the ShiftRows operation.


**3.Mix Column**: The MixColumns transformation operates at the column level. It transforms each column of the state to a new column. The transformation is actually the matrix multiplication of a state column by a constant square matrix. All the arithmetic operations are conducted in the Galois Field (Finite Field). The bytes are treated as polynomials rather than numbers. Figure shows the MixColumns operation.

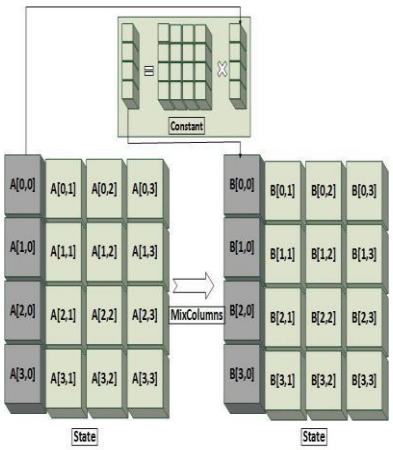
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

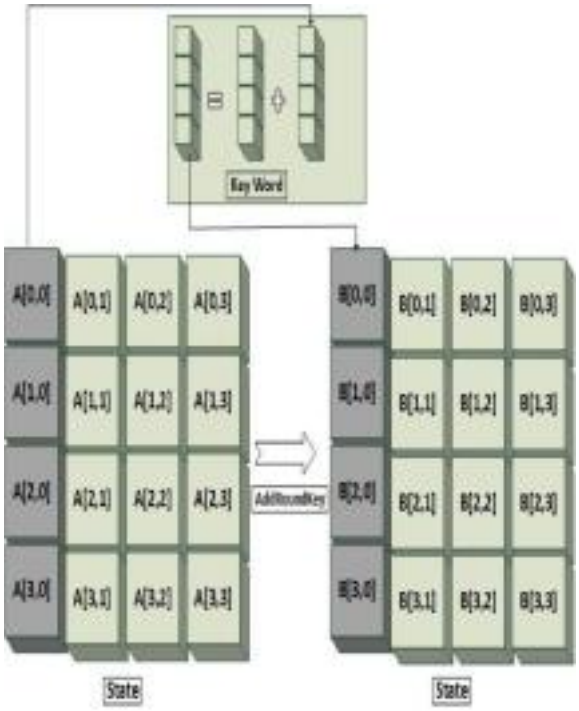
*Visit: www.ijirset.com*

**Vol. 8, Issue 3, March 2019**




**4. Add Round Key:** AddRoundKey proceeds one column at a time. It is similar to MixColumns in this respect. Ad-dRoundKey adds a round keyword to each column matrix. Matrix addition operation is performed in the AddRoundKey stage. Figure shows the AddRoundKey operation.

In encryption, SubBytes, ShiftRows, MixColumns, and Ad-dRoundKey are performed in all rounds except the last round



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

**MixColumns:** transformation operation is not performed in the last round of encryption. The decryption process essentially follows the same structure as the encryption, in addition to the nine rounds of Inverse Shift Rows, Inverse Sub Bytes, Inverse Add Round Key and Inverse Mix Columns Transformation. In the final round, Inverse MixColumns is no longer performed.

## V. MODIFIED ADVANCED ENCRYPTION STANDARDS

According to previous research observation, we have found out that S-Box and Mix Columns are the most energy consuming stages in encryption and decryption process. We have analyzed the S-Box generation process of the Rijndael AES. The 16x16 2-dimensional lookup table is formed through the multiplicative inverse phase and affine transformation phase in the original AES. We are proposing a new 1-dimensional lookup table as S-Box. It also follows the same generation process as the original one. However, substitution of one complete byte requires two times substitution from the S-Box. First four bits of the state byte is replaced first then the remaining four bits are substituted from the S-Box.

### A. Rijndael S-Box Generation Method:

The Rijndael S-Box is a square matrix which is used in the Rijndael cipher. The S-Box serves as a lookup table. It is generated by determining the multiplicative inverse for a given number in GF(28) and then transforming the multiplicative inverse using affine transformation.

**1) Multiplicative Inverse Phase:** In multiplicative inverse phase, the input byte is inversed by substituting value from multiplicative inverse table.

**2) Affine Transformation:** Selection of the irreducible polynomial and the designated byte are the two most important factors of affine transformation phase. In Rijndael AES, $x^8 + x^4 + x^3 + x + 1$ is used as the irreducible polynomial and as the constant column matrix 0x63 specially designated byte is chosen. Basically, the affine transformation consists of two operations. Firstly, 8x8 square matrix's multiplication and secondly, 8x1 constant column matrix addition.

The following figure illustrates the generation process of Substitution Box (S-Box) of the original AES.

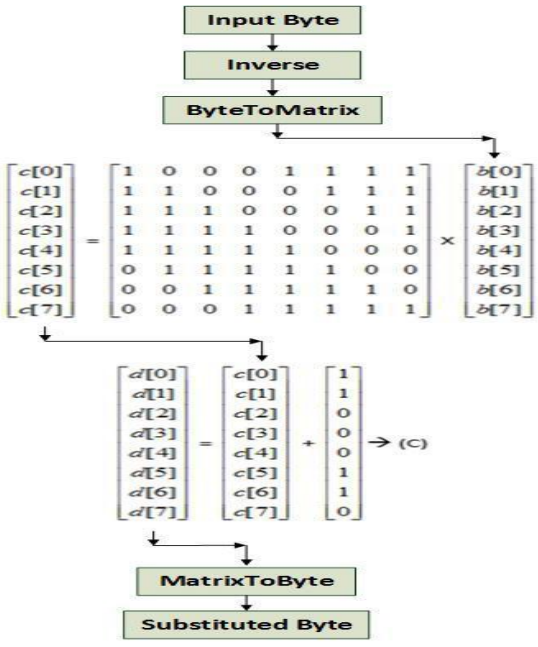



Fig: Substitution box of original AES

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

**B.Modified AES S-Box Generation:**

Our modified AES S-Box generation process follows the construction procedure of the original AES. The whole process differs only in the selection of the irreducible polynomial and specially designated byte.

**Multiplicative Inverse Table:** In the Rijndael AES, all the arithmetic operations are performed over the Galois Field (28). In our work, the Galois Field (24) is considered. The

number of irreducible polynomials of degree 4 over GF(2) are $x^4 + x + 1$, $x^4 + x^3 + x^2 + x + 1$ and $x^4 + x^3 + 1$.

All the generated values of the multiplicative inverse table and substitution box depend on the selection of irreducible polynomial. For our experiment purpose, we choose $x^4 + x + 1$ as our irreducible polynomial but we can select any of the

irreducible polynomials which are mentioned above. Following the Extended Euclidean Algorithm, 1 dimensional multiplicative inverse table is formed.

The following table illustrates the multiplicative inverse table of the proposed algorithm.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 9 | E | D | A | 7 | 6 | F | 2 | C | 5 | A | 4 | 3 | 8 |

Fig. Multiplicative inverse table

2) **Affine Transformation:** This affine transformation process also follows two phases. Firstly, 4x4 square matrix's multiplication and secondly, 4x1 constant column matrix addition. As we are calculating over the GF($2^4$) where the value of the constant column matrix ranges from 0x00 to 0x0F, we can only select 5 values from there as these values do not generate any fixed point after transformation. The fixed point refers to the generation of the output value same as the input value.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

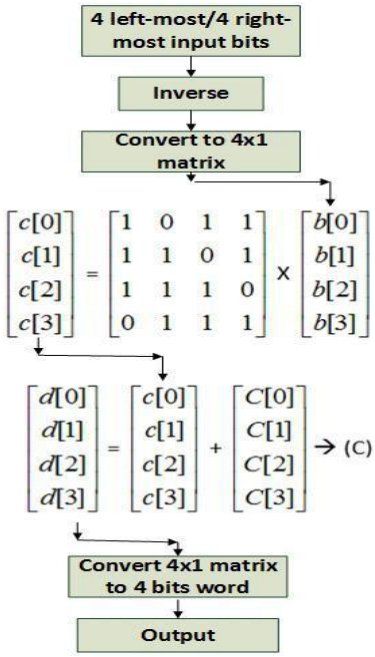
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

The following figure shows the generation process of proposed MAES.




Different S-Boxes and inverse S-Boxes for different values of the constant value C is given below :

Fig. Case-1: When C = 0x03

Case-1: When C = 0x03

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 4 | F | B | 2 | 1 | 7 | 0 | C | D | 5 | 9 | 6 | E | A | 8 |

Inverse S-box:

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 5 | 4 | 0 | 1 | A | C | 6 | F | B | E | 3 | 8 | 9 | D | 2 |

Fig. Case-2: When C = 0x08

Case-2: When C = 0x08

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8 | F | 4 | 0 | 9 | A | C | B | 7 | 6 | E | 2 | D | 5 | 1 | 3 |

Inverse S-box:

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | E | B | F | 2 | D | 9 | 8 | 0 | 4 | 5 | 7 | 6 | C | A | 1 |

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Fig. . Case-3: When C = 0x0A

Case-3: When C = 0x0A

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | D | 6 | 2 | B | 8 | E | 9 | 5 | 4 | C | 0 | F | 7 | 3 | 1 |

Inverse S-box:

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| B | F | 3 | E | 9 | 8 | 2 | D | 5 | 7 | 0 | 4 | A | 1 | 6 | C |

## VI. PERFORMANCE ANALYSIS

### A. Environment Setup:

To evaluate our experiment, we have gone through some environmental setup procedures. We have used telosB mote which is fully compatible with IEEE 802.15.4 standard and TinyOS 2.x. It has TI MSP430F1611 microcontroller and CC2420 RF chip. We implement MAES in nesC language which is supported in TinyOS 2.1.2. AA 1.5V batteries are used for the experiment. We integrate MAES in TelosB sensor motes then transmit the encrypted temperature data while the sensor motes are placed in two different locations. Then we run our experiment for a week and analyze the packet transmission rate, the energy consumption rate, and the latency of data transmission.

### B. Implementation:

As we propose a lightweight version of AES for RCEs, first analyze the actual mechanism of AES and implement AES in structured programming language before implementing it in nesC. The same process is followed for the proposed MAES. After implementing both the algorithms (AES and MAES) in nesC, we integrate these in telosB sensor mote. Humidity, temperature, and luminance can be sensed by telosB sensor mote. Room temperature is used as our input set for both the algorithms. Our experimental approach construct in two phases. In the first phase, we implement the original AES in the telosB sensor mote and construct two sets of transmitted data packets. The first data set is based on transmitting encrypted data packets using the original AES encryption techniques and the second data set is composed of without encrypted data packets. In the second phase, we implement both the original AES and the proposed MAES in the telosB sensor mote.

### C. Comparison:

The figure shown below illustrates the comparison between the number of packets of the first phase. Analyzing the result of figure , the black curve which is constructed from the original AES encrypted data set is steeped down compared with the red curve from the unencrypted data set. In this case, the voltage is dropped approximately from 1.48V (raw value = 4040) to 1.32V (raw value = 3600). The comparison between the number of packets of the second phase of our experiment is shown in figure below. As we have mentioned earlier, transmission of the unencrypted data packets are not considered in the second phase. From the data log, we analyze that 18915 packets are sent for AES encryption when the voltage is dropped approximately from 1.50V (raw value = 4096) to 1.30V (raw value = 3550). For the same amount of voltage degradation, 22385 packets are sent in terms of MAES which is significantly a better choice while working in RCEs. The efficiency rate is 18.35%. Our proposed algorithm gives more energy efficiency than the original one. We calculate the latency of the proposed MAES and compare the result with the original AES. We observe the time needed to transmit 1000 packets which are encrypted by both the original AES and the proposed

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

MAES. Considering the average transmission time, the latency of proposed MAES is less than the original AES. .

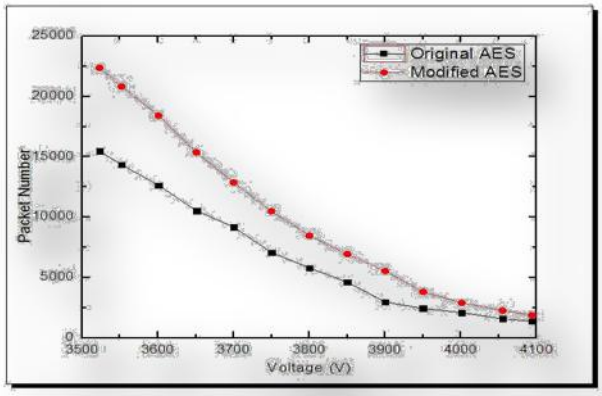



Fig.Number of packets comparison between the modified and the original algorithm.

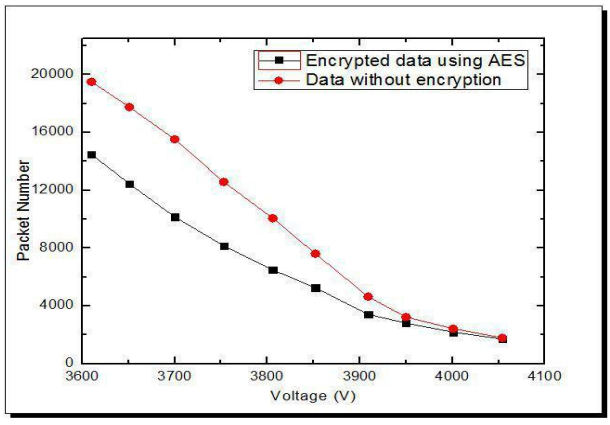



Fig.Number of packets comparison between the encrypted and the unencrypted data

**APPLICATIONS:**

It is used for confidentiality, authentication, data freshness, and data integrity might be extremely important.

It is used in Internet of Things (IoT), which is the next revolution of the internet which brings profound impact on our everyday lives.

It is used in Cryptography.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

The MAES algorithm gains wide application in our daily life, such as smart cards, cell phones, automated teller machines .

The M.O.S.T.(microprocessor operating system technology) Card C5 leverages the Advanced Encryption Standard (AES) for data encryption

The strongest encryption algorithm to date, so that our data will remain 100% confidential no matter where it is transmitted.

AES has typically been found on card operating systems that support public key infrastructure, but now users can get PKI security at the price of a symmetric key card.

## VII. CONCLUSION & FUTURE WORK

In this paper, we present a modified version

of AES for Resource-Constraint Environments. A new Substitution Box is proposed which works over the Galois Field ($2^4$) by constructing an unique affine transformation equation. One notable feature of MAES is extending the battery life of low powered devices by consuming less amount of energy. The proposed method shows 18.35% efficiency when encrypted packets are transmitted using the proposed MAES to the sink node and the number of transmitted packets has increased. In addition, 29.983 milliseconds is found in terms of latency. In future, the security issue and space complexity will be considered to make the proposed modification more applicable. Also, we plan to investigate multipath routing scheme while transmitting the encrypted data to the sink node. We will further delve to integrate Public Key Cryptosystem, specially Elliptic-curve cryptography (ECC) to achieve comparable efficiency in terms of number of packet transmission and latency with better security.

## VIII. ACKNOWLEDGMENT

Authors of this paper are extremely grateful to the anony-mous reviewers for their rigorous criticism about this work which help the authors to reorganize the work in excellence.

## REFERENCES

[1] Madakam, Somayya, R. Ramaswamy, and Siddharth Tripathi. “Internet of Things (IoT): A literature review.” Journal of Computer and Commu-nications 3, no. 05 (2015): p.164
[2] Bogdanov, Andrey, et al. “PRESENT: An ultra-lightweight block cipher.”CHES. Vol. 4727. 2007.
[3] Wu, Wenling, and Lei Zhang.“LBlock: a lightweight block cipher.” In Applied Cryptography and Network Security, pp. 327-344. Springer Berlin/Heidelberg, 2011.
[4] Al Hasib, Abdullah, and Abul Ahsan Md Mahmudul Haque. “A comparative study of the performance and security issues of AES and RSA cryptography.”Third International Conference on Convergence and Hybrid Information Technology, 2008. Vol.2.Wenceslao Jr, Felicisimo V., et al.“Modified AES Algorithm Us-ing Multiple S-Boxes.” The Second International Conference on Electrical, Electronics, Computer Engineering and their Applications (EECEA 2015)
[5] https://www.sciencedirect.com/science/ article/pii/S2212017316304959.html
[7] https://www.sciencedirect.com/science/article/pii/S2212017316304959.html
[8] https://pdfs.semanticscholar.org/de9f/bd d099760bd82f8bd4d15b0b23a796e8120 7.pdf.html
[9] https://searchsecurity.techtarget.com/def inition/encryption.html
[10] https://digitalguardian.com/blog/what-data-encryption.com
[11] https://www.tldp.org/REF/INTRO/Secu ringData- INTRO/encryption.html.com
[12] https://en.wikipedia.org/wiki/Advanced _EncryptionStandard.com
[13] https://medium.com/@pet3rpan/cryptog raphy-vs-encryption-1881606c400a.com
[14] https://www.springboard.com/blog/cryp tography-basics-the-ins-and-outs-of-encryption/.com
[15] http://www.cyber-rights.org/crypto/cryptog.html
[16] https://www.brighthub.com/computing/ enterprisesecurity/articles/65254.aspx.com
[17] https://cheapsslsecurity.com/blog/explai ned-hashing-vs-encryption-vs-encoding/.html
[18] https://ipfs.io/ipfs/QmXoypizjW3WknF iJnKLwHCnL72vedxjQkDDP1mXWo6 uco/wiki/Rijndael_S-box.html.com
[19] http://luca-giuzzi.unibs.it/html