International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1, October, 2019

An Efficient AES Algorithm for IoT based Applications

V.Nandan, R. Gowri Shankar Rao

Abstract: ***With a massive growth in net communications, there is always a chance of risk to keep the data secret, reliability of data, additionally accessibility of data. An outcome for this is gift cryptographic methodologies which includes the superior Encryption trendy (AES), which might be at gift shield such information, are necessitated to be quick and well protected. In this report, we talk two novel techniques for adapting the foresaid trouble and it is being made potentially through enhancing the design of mix column manipulation of Advance Encryption Standard (AES). An improvement of 1.27 occasions transformed into completed in evaluation to earlier calculations in expressions of pace proficiency [1][2]. As far as hardware structural layout, a space discount of almost thrice change is additionally achieved. AES has input data blocks of 128 bits, with keys length of 128,192 or 256 bits. In this manuscript, a hardware representation of AES algorithm is described using key of length 128 bits. The AES hardware set up is realized using xilinx nexys 4 artix 7 –FPGA board with the help of xilinx ISE design suite. Our work focuses on MAES, a low power AES encryption algorithm which run over the interest [5]. In MAES, a S-Box of one dimension is suggested using new mathematical expression for creating a (n×n) matrix in affine transformation. The percentage efficiency of 18.35% is obtained by MAES than AES, when encrypted packets are transmitted. Thus MAES expends low power compared to that of AES, which is suitable for resource constraint environments.***

Index Terms - AES, MAES, Substitution Box (S-Box), Artix–7 FPGA, power consumption, resource constraint environments (RCEs), Cryptography, TelosB.

I. INTRODUCTION

Novel upgrades are present in the world of technological know-how and equipment. A more noteworthy a piece of these innovations subject to the area of agribusiness, transportation, discussion and alike fields. Many of these innovations, which in cooperates mathematical algorithms, are set up on remote computer networks, utilizing the contemplations of wireless transmission and internet based remote server netoworks. [12] Advantageous wi-fi systems, utilize far off computers and virtual mystery networks additionally can be done. However, these sort of methods come close by means of their arrangement of endowments, the most extreme critical drawback which develop in the area of these structures are visible to unapproved entree, an attempt to exploit a computer system, phishing and furthermore in security breaks [1].

Revised Manuscript Received on October 30, 2019.

* Correspondence Author

V.Nandan*, Department of Elect & Comm Engineering Veltech Rangarajan Dr.Sagunthala R&D Inst. of science & Technology, Tamilnadu, India.

R. Gowri Shankar Rao, Associate Professor Department of Physics, Veltech Rangarajan Dr. Sagunthala R&D Inst. of science & Technology, Tamilnadu, India.

Consequently, a requirement arises for dealing with the protection of such systems, the usage of speedy, correct and effective methodologies and this has been attained by the use of cryptography [2]. The new upcoming innovation of the internet is Internet of Things (IoT). IoT is the expansion of the Internet to append pretty much the entire thing on the earth. It comprises of real physical objects varying from appliances of household to heavy machineries [1]. It makes objects themselves conspicuous, obtain intelligence, impart information about themselves and they can get to information that has been accumulated by different things [13]. What's more, they likewise refresh the communication network constantly with instantaneous data using the assistance of numerous sensors. Internet of things works with sensor nodes, radio frequency identification labels and so on. The components used in IOT have less calculation potential, limitation in memory capacity and power assets, in addition to vulnerability to physical capture. From the reference, Paper 1 studies about scalable task problem in cloud environment with the many relay selection strategies. Paper 2 presents a many Algorithms to handle Fully Homomorphic Encrypted Data on the Cloud. In paper 3 Secure Tensor Decomposition Using Fully Homomorphic Encryption Scheme. Progressive trust management for wireless sensor networks and its purposes to trust-based routing and intrusion detection are discussed in paper 4. The dynamic trust management for delay tolerant networks and its purpose to secure routing is examined in paper 5.

The most famous techniques available to perform cryptography are the advanced encryption general (AES), data encryption standard (DES) and Triple Data Encryption Standard (3DES). [5] In view of its endowments, the advance encryption standard is the most viable and popular over the other techniques [6]. This advance encryption standard (AES) algorithm, is also known as the Rijndael AES algorithm.

The major contribution of this document is

- Scope of data security is explained clearly.
- Many standard methods for data security in cloud using various domains are conversed with its merits and demerits.

The above said points obviously distinguish this survey from other surveys. It provides the detail as broad as former works. The document is arranged in the following order: Section II reviews the work related to scope. Section III converses relay selection methods from various domains. Section IV explains the performance analysis. Section V provides the possible conclusion.

II. OBJECTIVES:

At first, investigation of the real mechanism of AES is carried out using organized programming language and then it is executing in nesC. Similarly proposed MAES is also evaluated using constructed programming language and nesC. Next step is to integrate AES algorithms and proposed MAES algorithm in telos B sensor mote[8]. The input parameter such as room temperature is sensed by telosB for both the algorithms. Our methodology is examined in two stages. At the primary stage, two sets of transmitted data packets are produced by executing AES algorithm in the telosB sensor mote. The primary dataset is AES encrypted dataset and the second dataset is the data packets without encryption.

At next stage, the two algorithms such as AES and the proposed MAES algorithms are investigated in the telosB sensor mote. [5]. Similar to above discussed primary stage, two sets of transmitted data packets are collected. At this time, the original AES and the proposed MAES standards are utilized to encrypt the primary data packets of second stage. Unencrypted dataset are not measured in the second stage of the analysis.

The proposed MAES technique demonstrates 18.35% effectiveness while encrypted datasets are transmitted to the sink node and the amount of dataset transmitted is also more than the earlier. Additionally, 29.983msec with regard to latency is achieved. In the future, the problem of security and area intricacy will be assessed to make use of the suggested variation very appropriate.

III. SCOPE OF ENCRYPTION SELECTION

Recognizing confidential information using proposed algorithm

The algorithm requires an explicit block of bytes, outlined as identity block to discover the subsequent data of a confidential message.

1. **Hash cost**: It employ as an insignificant measure to verify and integrate. The hash value of dynamic message is retained and then later related while detaching the message. SHA1 hexadecimal value of length 40 digits is selected.

2. **Kind (extension) of report**: Despite the fact that the document has no development by any means, it will not create any issue as blankstring cost (“”) is aided.

3. **Key index**. For faster extraction of data, a zero-based index fee is essential to convey the application program, the stage at which the message sequence is being formed within the stego record. The value of it is equivalent to the extent of cover document. The perpendicular line/pipe (|) man or woman can detach the three values. Finally index key is generated and all the time lengthened that the whole duration of identification block is sixty four bytes. This block of ID undergo encryption process and soon after it is added to the completion of encrypted message [4].

Advance Encryption Standard

Advanced Encryption Standard (AES) algorithm is one of the symmetric encryption standards that were published by National Institute of Standards and technology (NIST) in 2000. It is the successor of Data Encryption Standard (DES), which cannot be considered as safe any longer, because of its short key with a length of only 56 bits. NIST invited experts who work on encryption and data security all over the world to introduce an innovative block cipher algorithm to encrypt and decrypt data with powerful and complex structure. From around the world many groups submitted their algorithm. NIST accepted five algorithms for evaluate. After performing various criteria and security parameters, they selected one of the five encryption algorithm that proposed by two Belgian cryptographers Joan Daeman and Vincent Rijmen. The original name of AES algorithm is the Rijndel algorithm. However, this name has not become a popular name for this algorithm instead it is recognized as Advanced Encryption Standard (AES) algorithm around the world.

AES has the ability to deal with three different key sizes such as AES 128, 192 and 256 bits and each of this cipher has 128 bit (16 bytes) block size. The key sizes decide to the number of rounds as shown in table 1.

Table 1. Size of Key and Number of rounds

Length of the Key	Number of Rounds(n)
128	10
192	12
256	14

For AES algorithm, the first input is divided into 4 operational blocks and stored in state matrix which is a ‘4X4’ byte matrix [1]. This AES algorithm is versatile and hence it can be mostly utilized in the programming language and physical hardware. Out of the three key length of AES algorithm, the key length of 128 bits is often utilized. At the point when under the length of the key, ten times of repeated calculation on inside the algorithm.

This method, replaces DES algorithm, to increase the data security [8]. The study employs block of 128 bits and key of length 256- bits. The round operation is the heart of Rijndael algorithm. Each round consists of the following operations, namely, Substitute Bytes(SubBytes), ShiftRows, MixColumns and AddRoundKey.

The following steps involved in the encryption process: 1) Initial Round: AddRoundKey

2) (n-1)Rounds: SubBytes, ShiftRows, MixColumns, and AddRoundKey. (where n relies on the length of the key)

3) Last Round: SubBytes, ShiftRows, and AddRoundKey

The algorithm undergoes Addround key operation at the beginning and end of the round operation.

AES Substitution Box:

SubByte is the most important module in Rijndael algorithm. SubByte is also referred as S-Box. It is a matrix consisting of hexadecimal values employed in the advance encryption algorithm. Substitution box is used as look up table. The SubBytes transformation is a non-linear byte substitution that operates independently on each byte of the State using a substitution table (Sbox). The SubByte is purposely chosen to be a nonlinear transformation as it provides a higher security services. This inverse Sbox, is constructed by composing two transformations

1. perform inverse multiplication for a given number in GF (28). Rijndael's finite field substitution box is produced as represented below,

GF (28) = GF (2) [x]/(x8 + x4 + x3 + x + 1) (1)

2. To alter the inverse multiplication, apply affine transformation.

This is a vector transformation in which XOR operation of the byte is considered.

The original AES uses five dimensions of units such as bits, bytes, characters, groups, states. From initial to final stage of encryption process, while changing from one segment to another segment of the data packet, the knowledge of AES uses data grouping. Design of AES algorithm should satisfy the following conditions:

(1)Resistance against all know attacks.
(2)Faster and compact coding.
(3)Design simplicity.

Analytical Framework of MAES; A first result is the advancement of a coherent analytical framework to be connected by the EU and its Member States so as to guarantee consistent methodologies are utilized. It is in this way outlined by wide set of key strategy questions. It is organized such that conceptual framework connects human social orders and their prosperity with the environment.

The main objective of this document is to find a efficient solution for real time implementation of AES algorithm to use of it at far places. AES algorithm is realised in xilinx ISE design suite. Xilinx Platform Studio (XPS) is a key component of the ISE Embedded Edition Design Suite, which helps the hardware designer to easily build, connect and configure embedded processor-based systems. XPS can possibly configure and assemble IPcores from Xilinx embedded IP catalogue. XPS and Xilinx software development kit (XSK) are integrated for realization of both hardware & software for a particular purpose [11].

Realization of MixColumn operation using Combined Shifter – LUT architecture

In mixcolumn operation, the multiplication of the resultant of shiftrow methods of AES with the MDS(Maximum Distance separable) matrices is carried out and is as shown in Fig. 2.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \quad \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$$

Additionally, for encryption process there is need for multiplying the inputs by numbers two, three, and one. Accordingly, if we have to adopt the LUT approach of the earlier part, then it is needed to store values equal to the numbers two, three and one. After several assessments, it is decided that LUT values for number one need not be stored as any assortment stretched out with 1 is the same comparable assortment. For multiplication with number 2, the values are stored just left shifting operation of plain single bit[16]. Therefore, it would be enough to store LUT values relevant to number 3 and thus with these adjustments; a major decrease in space is additional achieved.

Improved Vedic Math Method

In mixcolumn method, multiplication can be processed utilizing the equation explained in [14]. On the other hand, the best values of MDS matrices as in fig2 is such as 0x03 for encryption and 0x0E for decryption, will manifestly show that multiplicand needs less than 8 bits for characterisation. For this reason, the most extreme numeral of fractional multiplication created is lessened

Which in turn decrease space and execution speed.[15]

IV. ENCRYPTION SELECTION APPROACHES

A AES ALGORITHM AND APPEND INSERTION STEGANOGRAPHY TECHNIQUE FOR FILE ENCRYPTION AND CONCEAL APPLICATION

Steganography is a system of covering mystery correspondence in other safe looking article so its reality isn't uncovered. In this manuscript, a letter, that is a pc report of any kind, hide in a preferred cover or carrier report, that's a PC file of definite sorts. The steganography method employed on this manuscript is

termed as append insertion steganography approach. The technique of steganography is chosen as an exertion to get rid of the limit of message design, which proposes in masses of famous steganography techniques. AES-256 (Rijndael algorithm) is utilized to encrypt the concealed message with a confidential passphrase. An exceptional block of bytes is utilized

to recognize and authenticate the original message so it tends to be recouped while holding its reliability. In this paper, one cover document (file) encloses just only one message record. While carrying out testing, any 5 arbitrary files are employed as secret information (message) and the respective reliability is manipulated by SHA-256 in advance of hiding and succeeding of recuperation. During the process of testing, all of them preserve their reliability, established through particular hash values. Accordingly, the resulting application as the implementation of proposed algorithm is verified viable but only for individual usage, still several improvements needs to be implemented for wider usage. It is an another application for protection and security, which may smother what's more, counteract pointless of outsiders, as encrypted messages are recognizable despite the fact that they in drivel form. As a consequence, steganography may be functional to keep away from undesirable awareness or in sites where using the process of

encryption is unlawful. Encryption and steganography are jointly placed to assure that input data

is very secured. Some conceivable observer ought not to understand any endeavor of mystery conversation whatsoever, and while the existence of the message is adjusted, it is still not in significant frame. In digital steganography, data is being added at the end of the file. without causing any error, and it eradicates restrictions along with size and kind of records that is probably hide.

B. HYBRID METHOD FOR IMPROVEMENT OF AES SECURITY

Security is essential apprehension in facts coping with, broadcast, message broadcast and digital transfer on public data network. Cryptography (personal inscription) is the encryption system to convert messages to create facts safe as well as against assault.

Advance Encryption Standard is symmetric encryption benchmark preferred by National Institute of Standards and technology. Advance encryption standard is justified to be well protected, short and sturdy encryption algorithm. Advance Encryption benchmark is hired typically for the reason its fantastic capability and reputation. However in contemporary cyber-attacks are constantly increasing, consequently protection experts to live engaged inside the lab producing new methods to hold on invaders at howl. Brute- pressure jar, distinction harm, numerical harm and linear harm are feasible assaults on symmetric algorithm. In order to have the funds for sturdy security in data broadcast, AES algorithm using hybrid method of dynamic Key technology and dynamic Substitution box technology are usually recommended.

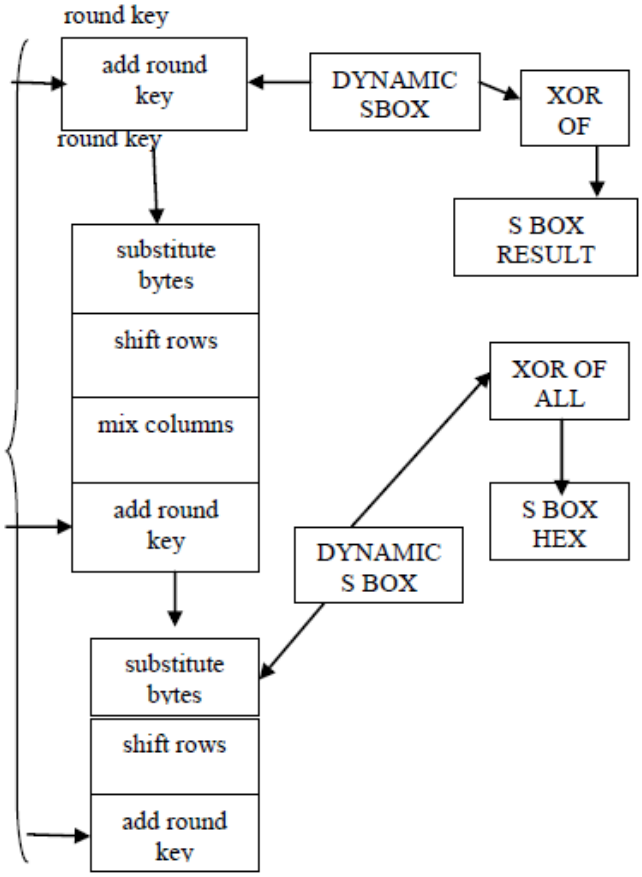

Fig.No. 1 S-BOX Generation

In hybrid method, we will upload greater composite in information to boost 'Confusion and Diffusion in Cipher text' through making use of dynamic Key technology and later using dynamic Substitution box technology. It can be made troublesome for assailant to have a look at constant set of Substitution box. Cryptography (mystery letter) is the ability and skill of altering messages to assemble statistics safe and opposed to assault. Encryption standard is to assure security of delicate statistics.

Encryption procedure performs bytes replacements and matrix changes at the plaintext (authentic record earlier than encryption) and adjustments the data into cipher text (random message). Security of data can be dealt with broadly accessible encryption algorithms. The decision of key is important in cryptography. The key selection decides the security of encryption algorithm. The most vital elements of encryption key are confidentiality and dimension of the key. A 'numeric or alpha numeric character' or completely unique symbol can be used as a key.

C. AES STANDARD FOR DIGITAL IMAGE ENCRYPTION

With the quick improvement of system and interaction machinery, digital image interaction has turn out to be an essential way of information broadcast. Consequently, additional concentration has to be taken for the improvement of the digital image encryption innovation. This manuscript, suggests encryption technology for a digital image using AES algorithm, and it is implemented in MATLAB simulation. At this point, execute digital image processing, attain the time to employ the advance encryption algorithm, unite the two methods. Subsequently, the encryption algorithm for the binary form of two dimensional image (digital image) is is realised in 'MATLAB Simulink'.

By the assessment of the bar chart investigation and the key investigation, it is observed that the methodology can represent the aftereffect of encryption and decryption in better way. By improvement in information technology, the transmit of image data safety is the main concern. During the process of transmit, the details of data may be interrupted by someone to hack, hence it is simple to transmit the drained information, the privacy of common people would be endangered. All of these are connected to the network of computer, has a solid link.

The Internet has small holes in the transmit of information security which is dangerous. 'Belgium cryptographers Joan Daemen and Vincent Rijmen' suggested advance encryption algorithm as encryption standard [11]. Advance encryption algorithm is quick as well as robust skill to withstand assaults [2] - [3], thus AES standard is broadly utilized in information encryption.

D. Advanced Encryption Standard Based on DNA computing technique

A novel method in cryptography study is DNA cryptography. It is based on computation of DNA field. Conventional 'cryptographic systems' are based on an efficient theoritical and arithmetical expression. DNA cryptography is developed to bridge the conventional and novel innovation. The computation effect of DNA cryptography will enhance the prevailing systems security which leads to the commencement of a hybrid cryptographic system.[17]. Our aim is to focus on DNA based design and realization of "Advanced Encryption Standard". AES algorithm is developed with all its requirements such as data, algorithms operations and used functions on DNA basis as substitute of bits. Thus a communication network for security enhancement is built on DNA basis, which is suitable for implementation in 'biological ecosystem' or on DNA computers. Therefore proposed algorithm retains security strength and stoutness of AES. 'Federal Information Processing Standards (FIPS)' authorizes cryptographic algorithm can be used to defend electronic information. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information [5], [6].

E. Description of Nexys 4 Artix -7 FPGA board

The Nexys 4 Artix-7 FPGA board is enhanced for high performance combinational logic computation. The Xilinx IC number used in our design is XC7A100T-1CSG324C. Nexys 4 board can host broader range of designs from introductory combinational circuits to influential embedded processors with several built-in peripherals (temperature sensors, I/O devices, accelerometer etc.), external memories, and compilation of USB, Ethernet, and other ports. Encrypted 7 series FPGA designs cannot be copied or reverse engineered for use on unintended FPGAs.

V. PROSPECT FORECAST

The volume of last assembly is around 58.5 KB. The testing of integrate experimental setup, is scrutinized to know whether the message file, (a file hidden inside the carrier/cover file), keep hold of its reliability in advance of self-encryption and fixed into the cover file, and afterward being effectively detached and decrypted. SHA-256 hash function creates hash value (it is also named signature or checksum).[13] The steady message record(file) will everlastingly create the comparative hash esteem. In this testing, five subjectively delivered records, each one with assorted size, got their hash esteem figured. Those reports was scrambled and hidden in a transporter record and afterward recouped back, utilizing the anticipated calculation portrayed in the past.

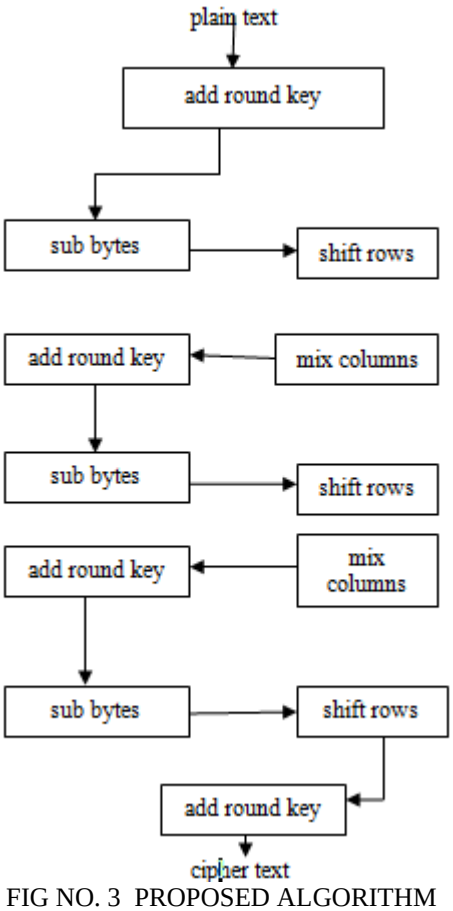

FIG NO. 3 PROPOSED ALGORITHM

As shown in Fig,1, in Rijndael algorithm, the input data undergoes one round of add round key, accompanied with 9 rounds of the 4 phases of the AES algorithm. Over close observation of different stages of 'AES algorithm' [8], it could be visible that the mixcolumn technique involves numerous mathematical manipulation and additionally takes long duration of time to compute [9].It happens so because, this mixcolumn step includes product of the input information with a previously calculated matrix called the Maximum Distance Separable.

An arbitrary portable document format (PDF) file sized around 2MB was utilized as envelop. The system will make use of data of 128 bits and length of the key is128 bits. The dispatcher will begin the procedure by message broadcast.

When sender logs in to system, the 'key' will be randomly engendered on basis of time value. In subsequently step, the value acquired after XOR on all bytes of round key, will execute rotational (circular) shift of it and thereby the substitution box will be made 'dynamic'. [8] To making S-box dynamic, additional phases has to be carried out. By employing cipher key, the static sbox will be converted into dynamic sbox in advance of substitute-byte transformation step. In similar way for the decryption process, inverse S-box will also be converted from static to dynamic S-box.

VI. CONCLUSION

The projected advance encryption algorithm with amalgam method will be an effectual method to offer robust security in message broadcast by increasing more composite to enhance confusion and diffusion in cipher text. The message will be protected from different attacks. The suggested system will be an efficient system for the purposes which are built on internet like e-commerce online shopping, stock buying and selling, net banking and electronic bill payment and so on. in adding, this technique lets the use of present regular aes to wreck the message/ concealed files. The appliance as the execution of projected model might be utilized to conceal and thereafter get back a note file, whose size will be around 47 mb in approximately 2.005 seconds.

REFERENCES

1. Mohit kumar, Apoorva singhal, 2012, "Efficient implementation of Advanced Encryption Standard (AES) for ARM based platforms", 1st International Conf. on Recent Advances in Information Technology, RAIT.
2. Yeong Chee Mei, Siti Zarina Md Naziri, 2011, "FPGA implementation of multiplicative inverse value of GF(28) generator using Extended Euclid Algorithm(EEA) method for Advanced Encryption Standard (AES) algorithm", International Conference on Computer Applications and Industrial Electronics (ICCAIE) , pp. 12-15.
3. Abdulrahman Moh'd et, al., 2011, "AES512:512bit Advanced Encryption Standard algorithm design and evaluation", 7th International conference on Information Assurance and Security (IAS), pp. 292-297.
4. S. Shivkumar, G. Umamaheswari, 2011, "Performance Comparison of Advanced Encryption Standard (AES) and AES Key Dependent S-Box - Simulation Using MATLAB 2011", International Conference on Process Automation, Control and Computing.
5. El-Sayed Abdoul-Moaty ElBadawy et. al., 2010, "A New chaos Advanced Encryption Standard (AES) algorithm for data security", ICSES.

6. Soufiane Oukili, 2017, "High speed efficient advanced encryption standard implementation",International Symposium on Networks, Computers and Communications (ISNCC).
7. Mark To Lock: 2017,"An image masking security application via insertion of invisible water mark using steganography and Advanced encryption Standard (AES)algorithm", International Conference on Applied System Innovation (ICASI).
8. Weiwei Shan, 2017, "Machine learning based side-channel-attack countermeasure with hamming-distance redistribution and its application on advanced encryption standard", Electronics Letters (Volume: 53, Issue: 14,).
9. He Fei, Gao Daheng, 2016, "Two kinds of correlation analysis method attack on implementations of Advanced Encryption Standard software running inside STC89C52 microprocessor", 2nd IEEE International Conference on Computer and Communications (ICCC).
10. Xiaokun Yang and Wujie Wen, 2017, "Design of a pre-scheduled data bus for advanced encryption standard encrypted system-on-chips" , 22nd Asia and South Pacific Design Automation Conference (ASP-DAC) , pp. 506-511.
11. Eddy Prasetyo Nugroho et. al., 2016, "SMS authentication code generated by Advance Encryption Standard(AES) 256 bits modification algorithm and One time Password (OTP) to activate new applicant account",2nd International Conference on Science in Information Technology (ICSITech).
12. Lokkireddi Phanikumar et. al., 2016, "Implementation of speech encryption and decryption using advanced encryption standard",IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) , pp. 1497-1501.
13. Berardino Carnevale et. al., 2016, "A flexible system-on-a-chip implementation of the Advanced Encryption Standard", 20th International Conference on System Theory, Control and Computing (ICSTCC).
14. Amruta R Dumane et. al., 2016, "Design of advanced encryption standard on soft-core processor", World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave).
15. Kishana Ram Kashwan el. al., 2015, "Improved serial 2D-DWT processor for advanced encryption standard", IEEE International Conference on Computer Graphics, Vision and Information Security (CGVIS), pp.209-213.
16. A. Nadeem el. al., 2016, "Performance Evaluation of Advanced Encryption Standard Algorithm", Second International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), pp.84-89.