**International Journal of Application or Innovation in Engineering & Management (IJAIEM)**
**Web Site: www.ijaiem.org Email: editor@ijaiem.org**
**Volume 6, Issue 6, June 2017 ISSN 2319 - 4847**

# Secure Data Transmission using AES in IoT

**Deepika khambra[1], Poonam Dabas[2]**

[1]M.tech Scholar: Department of Computer Eng. UIET, Kurukshetra University, Kurukshetra, India

[2]Assistant Professor: Department of Computer Eng. U.I.E.T, Kurukshetra University, Kurukshetra, India

## ABSTRACT

***Internet of Things (IoT) is a collection of billion of devices interlinked together to share information between them. As numbers of devices were increases the chances of security violation also increases because of presence of malicious nodes. Too securely transmission between two devices is challenging task. There are numbers of existing cryptography algorithms are available such as DES, RSA and AES. In this paper we provide secure data transmission mechanism in which we uses AES to increases the security of data. To implement propose mechanism we uses MATLAB and to analyse performance we uses metrics like execution time and throughput.***

**Keywords:** Internet of Things (IoT), Sensor, Attacks, Security and AES.

## 1.INTRODUCTION

The Internet of Things is turned into a prominent term for portraying situations in which Internet network and registering ability reach out to an assortment of articles, gadgets, sensors, and regular things. The Internet of Things is the interconnecting of millions of devices [1]. The Internet of Things (IoT) is a vital point in technology industry, strategy, and designing circles and has progressed toward becoming feature news in both the strength press and the well known media. This technology was epitomized in a broad range of organized items, frameworks, and sensors, which exploit progressions in processing power, hardware scaling down, and arrange interconnections to offer new abilities not already conceivable. A wealth of gatherings, reports, and news articles talk about and face off regarding the planned effect of the "IoT upset"— from new market openings and plans of action to worries about security, protection, and specialized interoperability. The vast scale execution of IoT devices guarantees to change numerous parts of the system we live [2].

### 1.1 Challenges of IoT

There are key challenges and implications today that need to be addressed before mass adoption of IOT can occur [3].

**1.1.1 Privacy and Security**: As the IoT roll interested in a key component of the Future Internet and the use of the Internet of Things for expansive scale, in part mission-basic frameworks makes the require to address trust and security works sufficiently.

**1.1.2 Cost versus Usability**: IOT uses technology to connect physical things to the Internet. For IOT adoption to grow, the cost of components that are needed to support capability such the same as sensing, tracking and control mechanisms need to be relatively inexpensive in the upcoming years.

**1.1.3 Interoperability**: In the conventional Internet, interoperability is the most fundamental centre esteem; the principal prerequisite of Internet availability is that "associated" frameworks include the power to "talk a similar dialect" of conventions and encodings. Distinctive enterprises today utilize diverse guidelines to support their applications.

**1.1.4 Data Management**: Data management is a crucial aspect in the Internet of Things. When consider a globe of things interrelated with continuously transfer all types of information, the amount of the generated information and the process involved in the handling of those data become critical [4].

### 1.2 Application of IoT

The IoT application covers “smart” environments/spaces in domains such as: Transportation, Building, City, Lifestyle, Retail, Agriculture, Factory, Supply chain, Emergency, Healthcare, User interaction, Culture and tourism, Environment and Energy. Below are some of the IOT applications [5].

#### 1.2.1 Internet of Smart Environment (IOsE)

Air Pollution checking: Control of CO2 emanations of processing plants, contamination discharged via autos and harmful gasses created in ranches, Forest Fire Detection: Monitoring of ignition gasses and pre-emptive fire conditions to characterize ready zones, Weather observing: climate conditions checking, for example, dampness, temperature, weight, wind speed and rain, Earthquake Early Detection, Water Quality: Study of water appropriateness in streams and the ocean for qualification in drinkable utilize, River Floods: Monitoring of water level varieties in waterways, dams and repositories amid blustery days, Protecting natural life: Tracking collars using GPS/GSM modules to find and track wild creatures and impart their directions by means of SMS.

### 1.2.2 Internet of Smart Health (IOsE)

Patients Surveillance: Monitoring of states of patients inside healing facilities and in old individuals' home, solutions and natural components, Fall Detection: Incapacitated individuals living autonomous, Dental: Bluetooth associated toothbrush with Smartphone application breaks down the brushing uses and gives data on the brushing propensities on the Smartphone for private data or for indicating measurements to the dental practitioner, Physical Activity Monitoring: Wireless sensors put over the bedding detecting little movements, such as breathing and heart rate and huge movements created by hurling and turning amid rest, giving information accessible through an application on the Smartphone.

This paper is divided into five sections. Section i presents introduction about IoT and its technical challenges and application, section ii covers literature review on various existing papers with their drawbacks, in section iii AES algorithm has been presented, section iv presents proposed work and at last section v shows results and analysis of paper.

## 2.RELATED WORK

Shah et.al.[6] proposed Home automation system based on loT used Reed Solomon codes to moderate risks and so enhancing security by providing error correction scheme both in the communication channel as well as the data store.

Venkata et.al[7] discussed a new light weight transport method(LWTM) which used existing Advanced Encryption Standard-Counter(AES_CTR) and Advanced Encryption Standard- Cipher block chaining (AES_CBC) algorithms in a approach to reduced computational time drastically for IoT applications involving large data.

Horton et al.[8] focused on the examination and enhancement of security between IoT enabled robots, specifically in this project, Turtle Bots, and the cloud infrastructure supported by them provided a combined set of security best practices for robotic file systems and communications.

Kuusijarvi etal.[9] discussed the current security challenges of loT devices and proposed a solution to secure these devices via a trusted Network Edge Device.

Shifa etal.[10] proposed lightweight encryption, which was preserve privacy and security of organizations and individuals by addressing the different levels of security required by multimedia applications at different phases in its operation.

Riahi etal.[11] proposed a systemic approach for IoT security. The model was completed of four nodes: person, technological ecosystem, process and intelligent object. The last node was the newest and reflects the IoT dimension.

Dalipi and Yayilgan[12] represented a comprehensive survey of the most recent contributions on security and privacy aspects of IoT applications in smart grid and identifies a number of the remaining challenges and vulnerabilities related to security and privacy.

Raghav etal.[13] proposed a straightforward information protection model wherever information was encrypted exploitation Advanced secret writing common place (AES) before it's launched in the cloud, so making certain information confidentiality and security.

Rao etal.[14] presented an AES implementation by using BRAM resources of newest Xilinx FPGAs. Total 08 dual port BRAMs were used to implement Byte Substitution operation of AES.

## 3.ALGORITHM USED TO SECURE DATA

Advanced Encryption Standard (AES): AES is symmetric key algorithm. AES used a block length of 128, 192, 256 bits. AES is base on top of permutation and substation network. AES used fixed block size. AES works on a 4x4 column-major order matrix of bytes. AES is fast in equally hardware and software implementation. AES provide very high/fast security. AES used low power consumption.

**Features of AES**

1. AES is a symmetric key symmetric block cipher.
2. AES is stronger and faster than DES.
3. AES give full specification and design details.
4. AES used larger key sizes.

**Operations of AES*:***

AES performs computations on bytes .AES used 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows. AES is variable depends on the length of key. An AES cipher specify the amount of repetitions of conversion rounds that exchange input that is called plaintext, and the final output is called ciphertext.

## PROPOSED WORK

In this section algorithm for encryption and decryption has been presented with their detail description. To enhance security of private keys different rounds will be performed to generate a private key.

**Algorithm of Encryption**

1)Start
2) Input data for encryption.
3) Transform/this data into hexadecimal number.
4) Now perform shift rows operation to transform this hexadecimal number into rows and column for encryption.
5) Perform mix column transformation to transform each column into a new column.
6)Now add some round key to each column to perform addition of matrix.
7) At last XOR the output of the addition of matrix with key.
8)Generate encrypted message.
9)End.

In this algorithm firstly input data is taken for encryption. After that transform this data into hexadecimal number and then perform shift rows operation to transform this hexadecimal number into rows and column for encryption. In Shift rows operation the initial queue is gone unchanged. Every byte of the next string is shift individual near the gone. In the same way, third and fourth queue be shifted. In shift rows transformation is a simple permutation. After that perform mix column transformation to convert each column keen on an original line. In column conversion make original column standards by apply expressions to convert input column. An expression is able to contain variables, function, operator and column from the transformation input. And then add some round key to each column to perform addition of matrix. At last XOR the output of the addition of matrix with key. XOR is exclusive or exclusive disjunction is logical operator.

**Algorithm for Decryption**

1) Start
2) Input data for decryption.
3) Transform/this data into hexadecimal number
4) Now perform shift rows operation to transform these hexadecimal numbers into rows and column for decryption.
5) Perform mix column transformation to transform each column into a new column.
6) Now add some round key to each column to perform addition of matrix.
7) At last XOR the output of the addition of matrix with key.
8) Generate original text.
9) End.

In this algorithm firstly input data is taken for decryption. After that transform this data into hexadecimal number and then perform shift rows operation to transform this hexadecimal number into rows and column for decryption. In Shift rows operation the initial queue be gone unchanged. Every byte of the next string be shift individual near the gone. In the same way, third and fourth queue be shifted. In shift rows transformation is a simple permutation. After that perform mix column transformation to convert each column keen on a original line. In column conversion make original column standards by apply expressions to convert input column. An expression is able to contain variables, function, operator and column from the transformation input. And then add some round key to each column to perform addition of matrix. And at last XOR the output of the addition of matrix with key. XOR is exclusive or exclusive disjunction is logical.

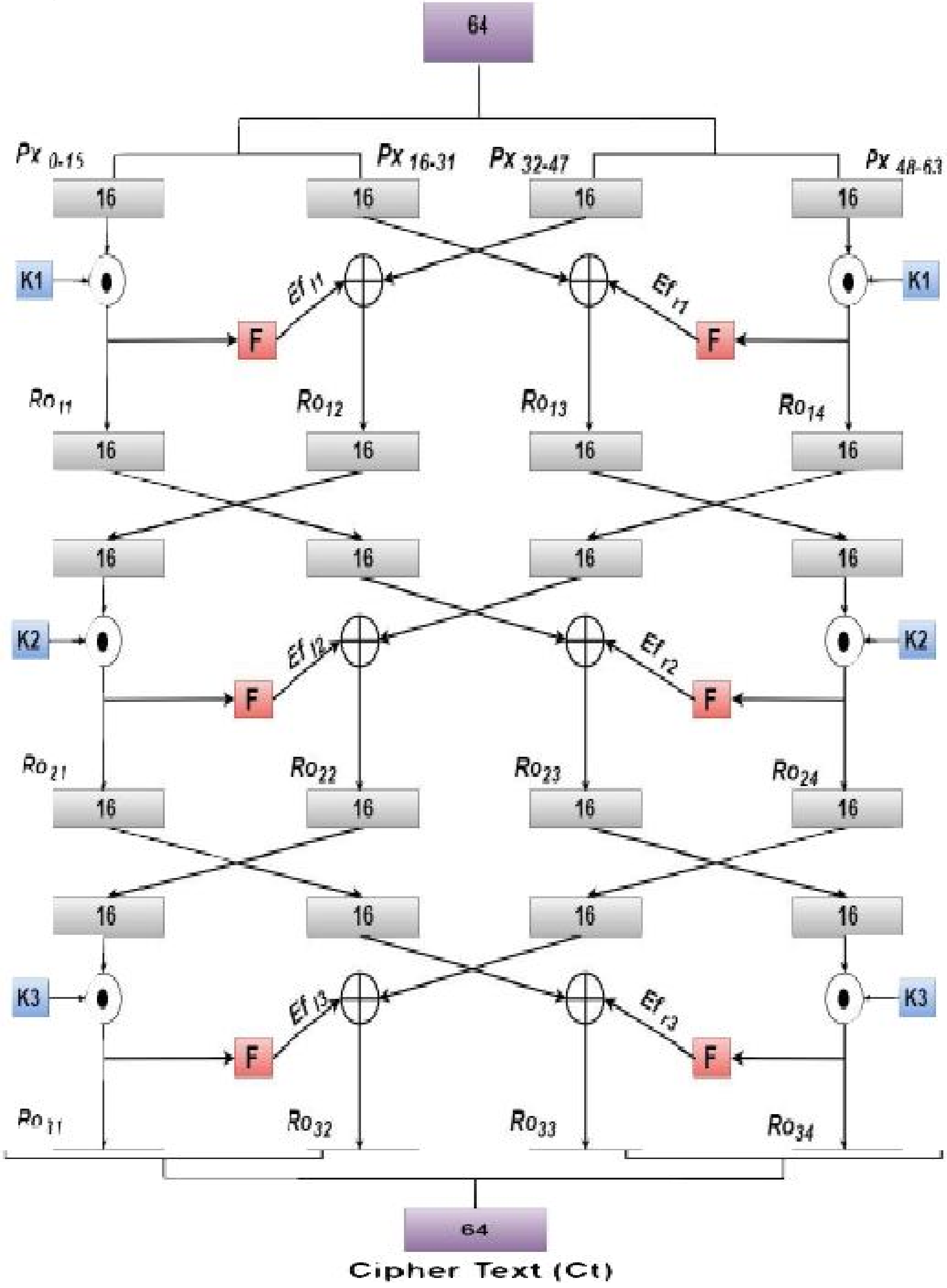

**Fig 1** System model of proposed work

Fig.1shows working of proposed mechanism. So to solve this here in this section we presented our proposed mechanism. In proposed mechanism increase throughput and execution time with AES. AES (advanced Encryption Standard) used 64 bit key mechanism to perform encryption and decryption on data before sends one device to another. After the generation of round keys the encryption process can be started. For the purpose of creating confusion and diffusion this process is composed of some logical operations, left shifting, swapping and substitution. The method of encryption is for the first round an array of 64 bit plain text (pt) is first faceted into four segments of 16bits. As the bits progresses in each round the swapping operation applied so as to diminish the data originality by altering the direct of bits, essentially increasing confusion in cipher text. Bitwise XOR operation is performed between the respective round key Ki. After processing every one key of a strong cipher key will be generated by the combinations of all four keys.

## 4.RESULTS AND ANALYSIS

Tool used: to analyse proposed mechanism we uses MATLAB. MATLAB is a matrix laboratory. MATLAB is a muti-paradigm numerical computing environment and fourth generation programming language. A programming language developed by MathWorks.

Performance Matrices:

a) Throughput: It depicts amount of message successfully delivered in perspective of whole amount of messages created towards destination within given time.

b) Execution Time: It depicts the whole amount of time taken by device to perform successful transmission of messages in IoT.

**Table 1:** Simulation Parameters

| Parameters | Values |
|---|---|
| Simulation Area | 100X100 |
| Number of Nodes | [100;200;300] |
| Rounds | 50 |
| Inital Energy | 0.5 J |
| Operating System | Windows 7 |

**Table 2:** Throughput of without AES and Proposed Mechanism

| Number of nodes | 100 | 200 | 300 |
|---|---|---|---|
| **Without AES** | 1.7102 | 2.6391 | 3.0638 |
| **Proposed** | 2.8630 | 4.2553 | 5.2632 |

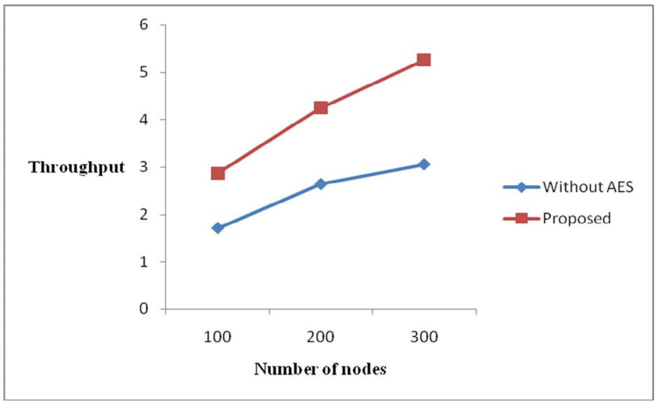

**Figure 2**Throughput v/s Number of Nodes

**Table 3:** Execution time of without AES and Proposed Mechanism

| Number of nodes | 100 | 200 | 300 |
|---|---|---|---|
| Without AES | 10.2239 | 13.2843 | 18.2878 |
| Proposed | 76.5304 | 80.8851 | 85.7570 |

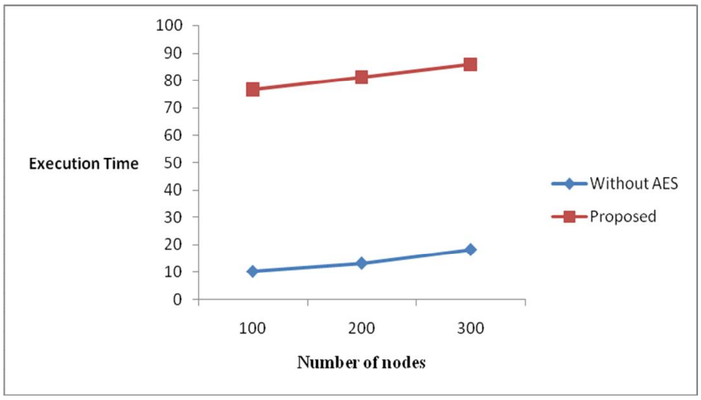

**Figure 3** Execution v/s Numbers of Nodes

Fig 2 shows depicts throughput of proposed mechanism and default routing process of IoT without AES which is measured by varying number of nodes from 100 to 300. In proposed mechanism throughput is high as compare to default routing without AES.

## 5.CONCLUSION

Secure data transmission between IoT is a very challenging task. There are numbers of existing algorithms available that provides secure data transmission out of them AES is much secure then other algorithms. On the basis of these algorithms, in this paper we provide mechanism which uses enhanced AES algorithm in which number of rounds or generation of private key increases that will help in generation of more secure encrypted key through which devices can transmit data in secure manner. Results show that in our mechanism throughput of data transmission system increases. In future try to enhanced proposed mechanism and focus on reducing end to end delay occurred during secure data transmission.

## REFERENCES

[1] Ovidiu Vermesan SINTEF, Norway, Peter FriessEU, Belgium, “Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems”, river publishers’ series in communications, 2013.

[2] Ovidiu Vermesan SINTEF, Norway, Peter Friess EU, Belgium,“Internet of Things–From Research and Innovation to Market Deployment”, river publishers’ series in communications, 2014.

[3] Martín Serrano, Payam Barnaghi, Francois Carrez Philippe Cousin, Ovidiu Vermesan, Peter Friess, “Internet of Things Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps”, European research cluster on the internet of things, IERC,2015.

[4] Karen Rose, Scott Eldridge, Lyman Chapin, “The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World”, The Internet Society (ISOC), 2015.

[5] Karen Rose, Scott Eldridge, Lyman Chapin, “The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World”, The Internet Society (ISOC), 2015.

[6] Idris Afzal Shah,Faizan Amin Malik and Syed Arshid Ahmad, “Enhancing Security in loT based Home Automation using Reed Solomon Codes” IEEE WiSPNET 2016 conference pp:1639-1642.

[7] Sainandan Bayya Venkata, Prabhakara yellai, Gaurav D verma, Andhavarapu Lokesh, Aditha KS and Siva Sankara Sai Sanahapati, “A new light weight transport method for secured transmission of data for Internet of Thing,” 10.1109@AICCSA.2016.7945813.2016IEEE .

[8] Michael Horton, Lei Chen and Biswanath Samanta, “Enhancing the Security of IoT Enabled Robotics: Protecting TurtleBot File System and Communication”, Workshop on Computing, Networking and Communications (CNC) IEEE 2017, pp: 1-5.

[9] Jarkko Kuusijarvi, Reijo Savola, Pekka Savolainen and Antti Evesti, “Mitigating loT Security Threats with a Trusted Network Element”, The 11th International Conference for Internet Technology and Secured Transactions (ICITST-2016), IEEE pp:260-265.

[10] Amna Shifa, Mamoona N. Asghar and Martin Fleury, “Multimedia Security Perspectives in IoT”, Sixth international Conference on Innovative Computing Technology, IEEE 2016 pp: 550-555.

[11] Arbia Riahi, Yacine Challal, Enrico Natalizio, Zied Chtourou and Abdelmadjid Bouabdallah, “A systemic approach for IoT security”, IEEE International Conference on Distributed Computing in Sensor Systems, 2013 pp: 351-355.

[12] Fisnik Dalipi and Sule Yildirim Yayilgan, "Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenges", 4th International Conference on Future Internet of Things and Cloud Workshops2016, pp: 63-68.

[13] Prasoon Raghav, Rahul Kumar and Rajat Parashar, "Securing Data in Cloud Using AES Algorithm", International Journal of Engineering Science and Computing, 2016, ISSN 2321 3361,pp: 3672-3675.

[14] Muzaffar Rao, Thomas Newe and Ian Grout, "AES implementation on Xilinx FPGAs suitable for FPGA based WBSNs", Ninth International Conference on Sensing Technology, IEEE 2015, pp: 773-778.