IMPROVING COMMUNICATION SECURITY IN IOT USING HYBRID ENCRYPTION DECRYPTION

D.M.Trivedi[1], Prof. T.J.Raval [2],

[1] *Student, Computer Engineering, L. D. College of Engineering, Gujarat ,India*
[2] *Prof T.J.Raval, Computer Engineering ,L. D. College of Engineering, Gujarat ,India*

ABSTRACT

Internet of Thing is the emerging technology in the field of Computer Engineering especially in networking field. Where networking may consist of the internal or external network. The Internet is the backbone of the IOT. And IOT is the technology where electrical, mechanical objects may be connected to the internet to control them remotely from anywhere of the world. Useful data and information will be swapped by billions of devices and services and these services and devices will be powered by Internet of Things. As IOT systems will be ubiquitous and pervasive, a number of security and privacy issues will arise. And the things which are connected to the internet may have many security concerns. Due to security and privacy related concerns, IOT could not set himself as a reliable technology.

Keyword : - *Internet of Thing , Encryption, Decryption, Avalanche Effect*

1. INTRODUCTION

Internet of Thing is used widely in the world, because of the requirement of smart Devices, in various field like water, health, transport to reduce human intervention and improve performance, but this is also the main scope for hackers, so we need to protect the system from cyber attack, thus the requirement of secure data is most important, to provide confidentiality, integrity and authenticity hybrid approach is better. the proposed system is based on hybrid encryption decryption technique to secure data.

1.1 Hybrid System

In this proposed system the benefit of symmetric and asymmetric algorithm is taken into consideration,The symmetric algorithm is AES and the Asymmetric algorithm is NTRU (Nth Degree Truncated Polynomial Ring Unit) ,the combination of these two algorithms are used .

2. Encryption using Proposed System

As shown in the figure 3.1 that First the Random Sequence has been generated, it has been used as key to encrypt Data of AES,AES is the Symmetric algorithm ,the main drawback of symmetric algorithm is the key exchange must be in secure manner, that has to be overcome in proposed algorithm with NTRU 's public key to encrypt that random sequence that has been used as secret key for Encryption and Decryption of Sensor Data. the encrypted message and encrypted key has been delivered to receiver.

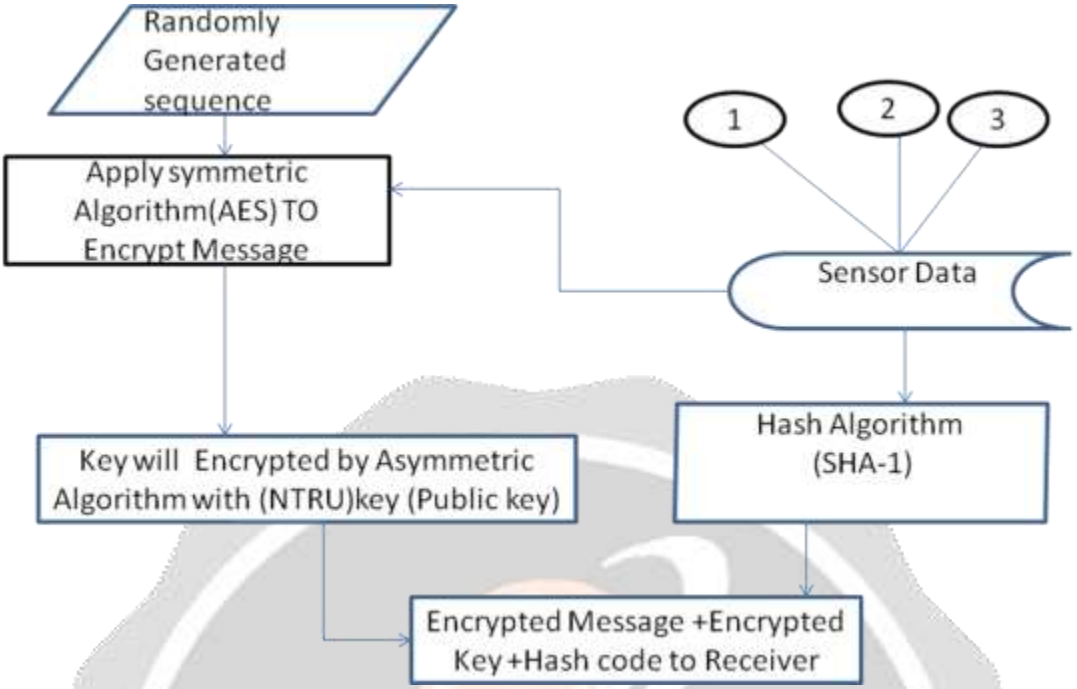

Figure 1: Encryption Process

3.2 Decryption Process in Proposed System

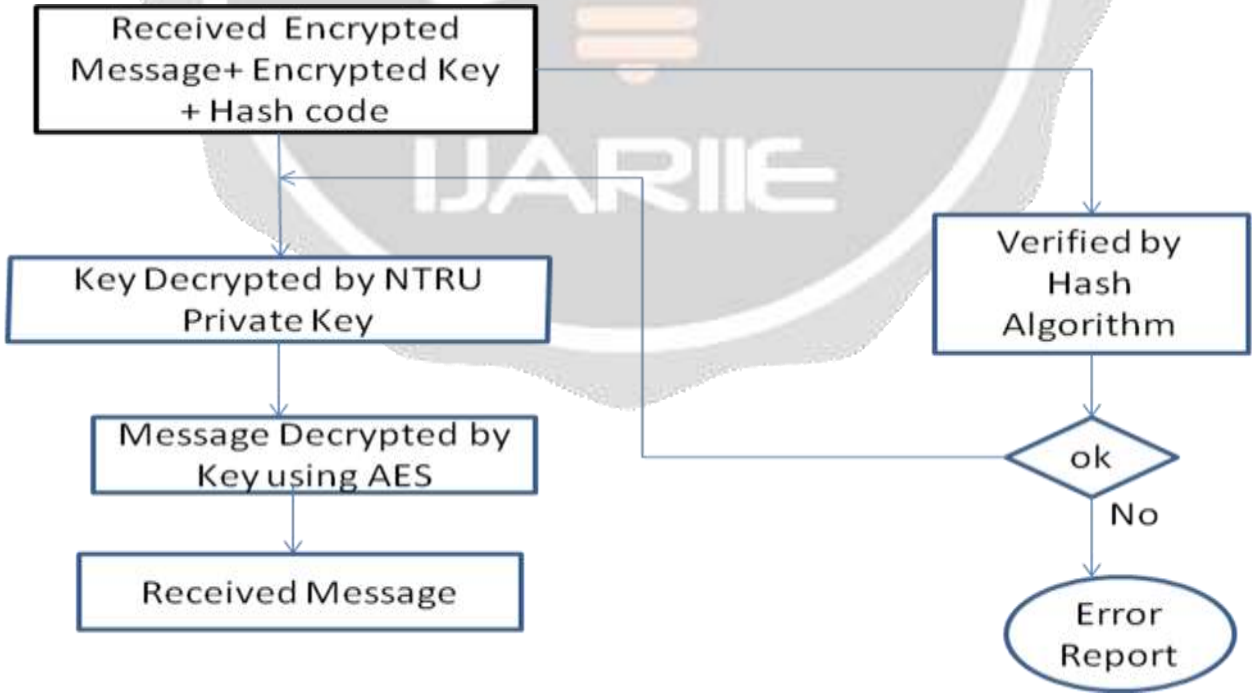

Figure 2: Decryption Process

The receiver will receive the Data in the encrypted format, receiver first verify the hash and then if the verification is not proper then generate error report else decrypt the key using NTRU 's Private key , and with use of this key receiver will decrypt the data.

3. Experimental Parameters

a) Encryption time: The time which has been taken by algorithm to encrypt the plaintext into cipher text.

b) Decryption Time: the time which an algorithm takes to decrypt the cipher text into plaintext.

c) Avalanche Ratio: The Ratio of the number of bit change /total number of bits in the file.

4.Implementation Environment

About Tools

Raspberry Pi is the single board compute developed in UK for making projects in developing countries, it is particularly design for smart devices which takes the input from the sensor and creates the machine –machine communication without any interference of human being

The Raspberry pi Foundation have analyzed that about 10 million user will be there in 2020.

There are various generation of raspberry pi has been released. First was Raspberry pi 1 Model B then B+, PI II Model B etc are available.

Now a latest model of raspberry pi are available with wifi ,Bluetooth ,USB boot capabilities

Language specification

Proposed system has been developed in java language because of its platform independent feature. it helpful in making application that write once runs everywhere. so it is helpful in embedded type o application also.

5.Experimental Results

5.1 Result of Encryption Decryption File

Sample Input File

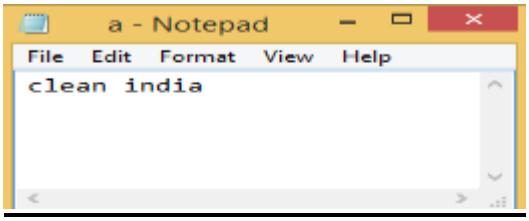

Figure 3 Sample Input File

Encrypted File of Sample Input File

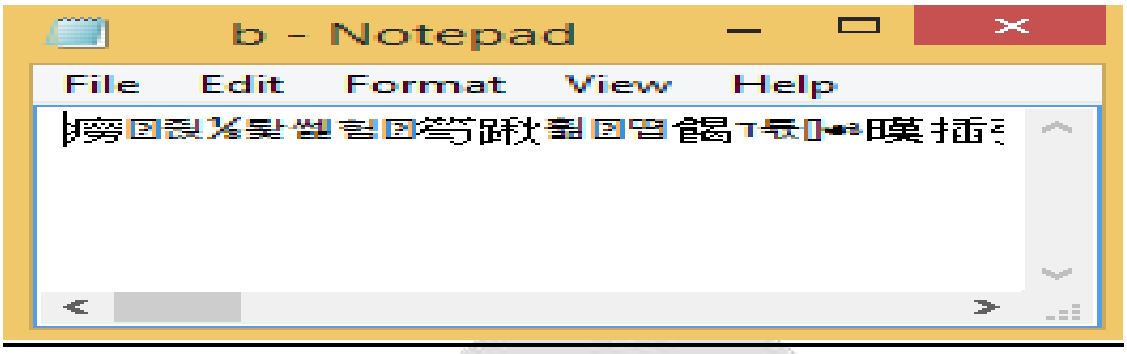

Figure 4 Encrypted File of Sample Input File

Decrypted File As Output File

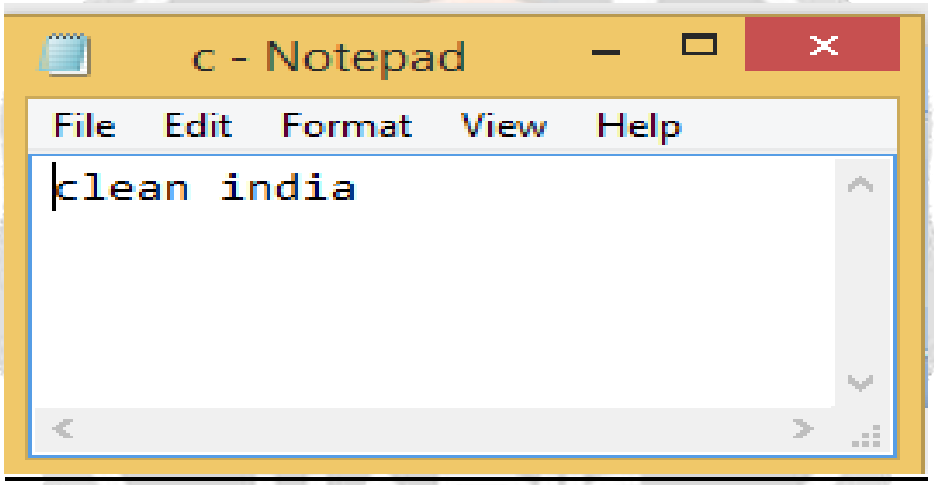

Figure 5 Encrypted File of Sample Input File

Execution time of various size of file using proposed Encryption algorithm

```
Execution time is 1769 miliseconds
ypt a.txt b.txt

Key generation time is 42 miliseconds
Execution time is 1374 miliseconds
pi@raspberrypi:~/ME $ java SampleAESNTRU -encrypt 10k.txt e10.txt

Key generation time is 42 miliseconds
Execution time is 1380 miliseconds
pi@raspberrypi:~/ME $ java SampleAESNTRU -encrypt 20k.txt e20.txt

Key generation time is 42 miliseconds
Execution time is 1399 miliseconds
pi@raspberrypi:~/ME $ java SampleAESNTRU -encrypt 50k.txt e50.txt

Key generation time is 42 miliseconds
Execution time is 1396 miliseconds
pi@raspberrypi:~/ME $ java SampleAESNTRU -encrypt 100k.txt e10.txt

Key generation time is 42 miliseconds
Execution time is 1413 miliseconds
ypt 100k.txt e100.txt

Key generation time is 42 miliseconds
Execution time is 1452 miliseconds
```


Various File size Execution time in milliseconds								
Algorithm	1k	(10K)	20k	50k	100k	200k	500k	1000k
AES Encryption	1277	1298	1305	1303	1312	1328	1369	1434
AES Decryption time in milliseconds	1290	1318	1345	1372	1390	1421	1505	1641
RSA Encryption	18809	NA	NA	NA	NA	NA	NA	NA
RSA Decryption	19060	NA	NA	NA	NA	NA	NA	NA
Proposed Encryption + Hash Code	1369	1380	1399	1396	1452	1454	1502	1588
Proposed Decryption + Verification Hash Code	1380	1397	1420	1491	1460	1476	1535	1604

Table 1:Various files execution time with various algorithm

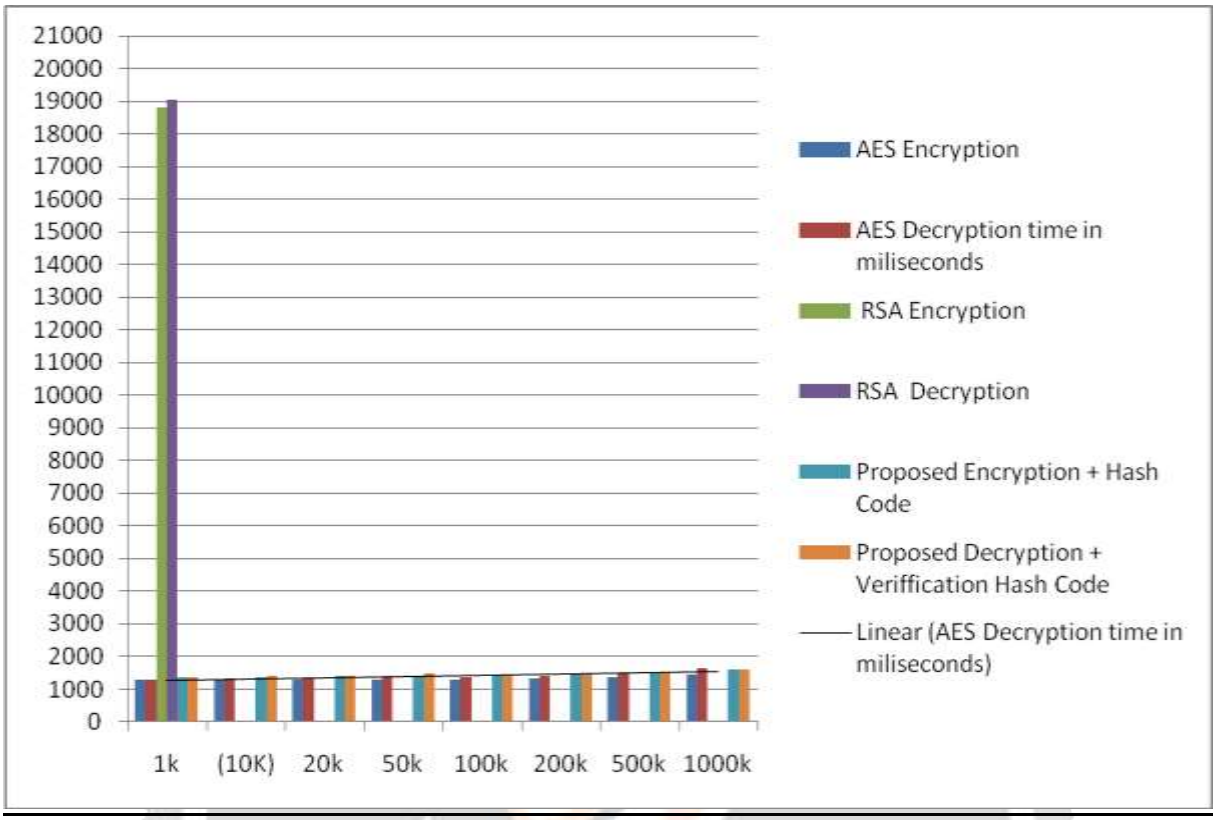

Chart1: Execution time of various size sample Input File with various algorithm

Avalanche Effect	
Algorithm	Avalanche ratio
AES	46.09
RSA	50.04
Proposed	50.09

Table:2 Avalanche Effect

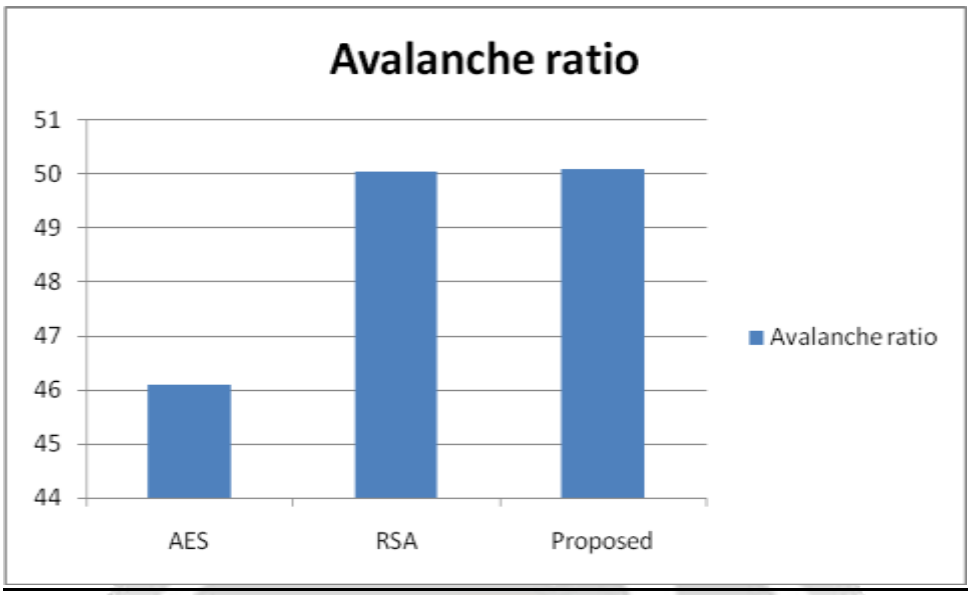

Chart 2 : Avalanche Ratio

6. CONCLUSIONS

The proposed algorithm will provide the Authenticity, confidentiality and Integrity with the benefit of faster Symmetric algorithm AES for Data Encryption while Most Secure public key cryptosystem NTRU and hashing algorithm.

- The proposed algorithm will be compatible for future generation also.

Limitation:

- The execution time will increase than that of single algorithm.
- Continuous internet connection is required.

Future Work

The proposed system will work for various types of files also. The proposed system may useful for e-voting ,e-commerce using IOT. Where the security is major concern**.** The various parameters like power consumption energy requirement will also consider.

7. REFERENCES

Web References:

[1] markups.kdanmobile.com/sharing/

[2] Joe Ruether, Cryptography Primer, http://jrruethe.github.io/blog/2014/10/25/cryptography-primer/

Book References:

[1] William Stallings, "Cryptography and Network Security: Principles & Practices", 4th edition, Prentice Hall, ISBN: 978-0-13-187316-2, 2005.

[2] Atul Kahate ,"Cryptography and Network Security:

Research Paper/Journal References:

[1] Mingyuan Xin,2016 , **"**A Mixed Encryption Algorithm Used in Internet of Things Security Transmission**"** International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery

[2] T K Goal," Lightweight Security Algorithm for Low Power IoT Devices, (ICACCI), Sept. 21-24, 2016

[3] S. Singh**,** 2017,"Advanced lightweight encryption algorithms for IOT devices: Survey, challenges and solutions"**,** © Springer-Verlag Berlin Heidelberg

[4] A. Safi, 2017," Improving the Security of Internet of Things Using Encryption Algorithms", International Scholarly and Scientific Research & Innovation 11(5)2017

[5] S Koteshwar,2016 "Comparative study of Authenticated Encryption" Targeting lightweight IOT applications, 2168-2356 (c) 2016 IEEE,

[6] Dr. S. S. Manikandasaran, 2016,"Security Attacks and Cryptography Solutions for Data Stored in Public Cloud Storage" (IJCSITS), ISSN: 2249-9555 Vol.6, No1, Jan-Feb 2016