JNNCE Journal of Engineering & Management, Volume 6, No.1, Jan – June 2022 ISSN 2582-0079
This paper is presented at National Workshop on Cryptology NWC 2021, held at JNN College of Engineering, Shimoga during 18-20 Nov 2021

Available online @ https://jjem.jnnce.ac.in
https:www.doi.org/10.37314/JJEM.2022.060117
Indexed in International Scientific Indexing (ISI)
Impact factor: 1.395 for 2021-22
Published on: 31July 2022

Light Weight Cryptographic Algorithms - A Comparison for IoT Sensor Data

Latha P[1]*, Andhe Pallavi[2]

[1*,2] Dept of Electronics and Instrumentation, RNSIT, Bengaluru,

Latha.saanvi@gmail.com, pallavi_ap@yahoo.com

Abstract

Transactions done online everyday are generating terabytes of information data. Securing this information over the internet is a challenging task. Cryptography plays a major role in securing this data and providing confidentiality to authenticated and genuine users. Various parameters such as encryption time, decryption time, memory consumption, weakness and strengths are to be evaluated before choosing the right algorithm. IoT devices are constrained in their resources. Light weight cryptographic algorithms are meant for such resource constrained devices. This paper gives a comparative study of few light weight cryptographic algorithms. This paper also discusses the encryption and decryption of data collected from IoT sensor and their performance evaluation

Keywords: *Blowfish, TEA, RSA, DES, AES*

1. Introduction

The number of devices connected over the internet is increasing day by day. Trillions of these devices generate huge amount of data. Security of this data is a major thing to be addressed. Cryptographic techniques are employed to secure this data. The encrypted data is in an unreadable format. Decryption retrieves back the information in the original format.

Data collected from IoT sensors which are class0 devices are very small in size. Since these devices are resource constrained, light weight cryptographic algorithms can be used to provide the security.

2. Cryptographic Algorithms

The cryptographic algorithms used to secure the data generated are either symmetric or asymmetric type.

Symmetric type in which the key used is common (secret key) between the sender and the receiver. This common key has to be shared between the two entities even before transmission. The strength of the encryption depends on the size of the key chosen. Longer the key size, harder it is to break.

Asymmetric type algorithms use different keys at the sender and the receiver side. A public key is used at sender side and a private key is used at receiver side.

3. Implementation of Encryption and Decryption

Bosch XDK device supports several sensors like temperature, humidity, pressure, Gyroscope, magnetometer and others. IoT sensors, which are mainly class 0 devices, provide data which are few bytes. The IoT sensors considered here at temperature and humidity sensors.

Class 0 devices are those which have limited resources like RAM size is less than 1KB and Flash size is less than 100KB

BME280 is the device which incorporates temperature, and humidity sensors. The humidity sensors are designed especially for wearable's and mobile applications mainly with low power consumption (resource constrained devices). It also provides high accuracy and long term stability. The sensor data collected is taken in an excel file.

The excel data is encrypted using light weight cryptographic algorithms-Blowfish and TEA. The encrypted data is transmitted to the client side using hivemq which is MQTT protocol. The received data at the client side is decrypted using Blowfish and TEA. The parameters considered for evaluation are RAM size, encryption time, decryption time, memory requirement. The implementation is done using the JavaScript Node.js

3.1 Blowfish algorithm

Figure 1 shows the computation of Blowfish algorithm. The IoT sensor data in the excel file is read line by line and encrypted using Blowfish algorithm. For implementing the algorithm, the data is taken as blocks of 64 bits. The number of iterations used here is 16. The substitution boxes used are 4 in number. The encryption is as follows.

3.2 TEA (Tiny Encryption Algorithm)

Figure 2 shows the computation of TEA algorithm. The TEA algorithm reads every line of excel data and encrypts taking 64 bit blocks and 128 bit key. After 32 rounds of iterations it produces the cipher text. The TEA encryption is shown as

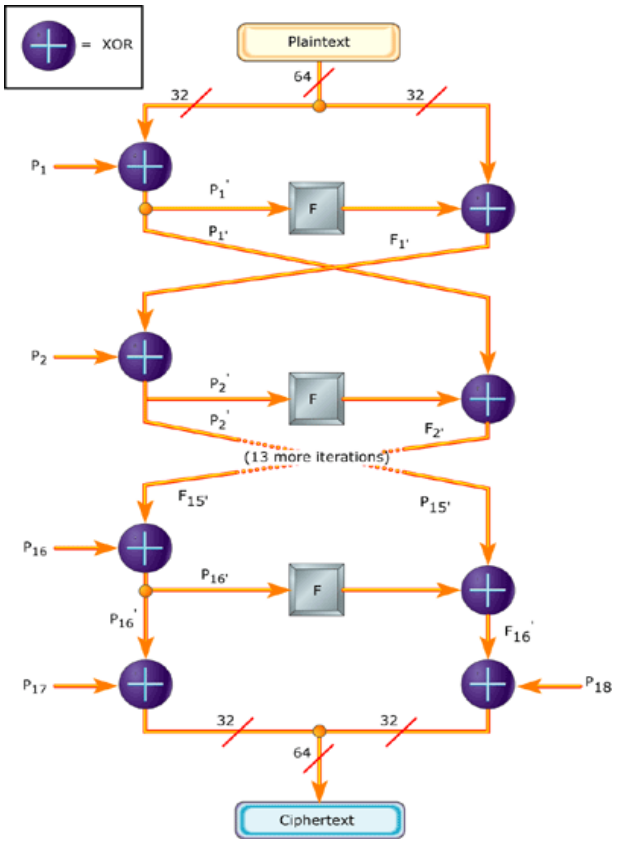


Figure 1: Computation of Blowfish algorithm

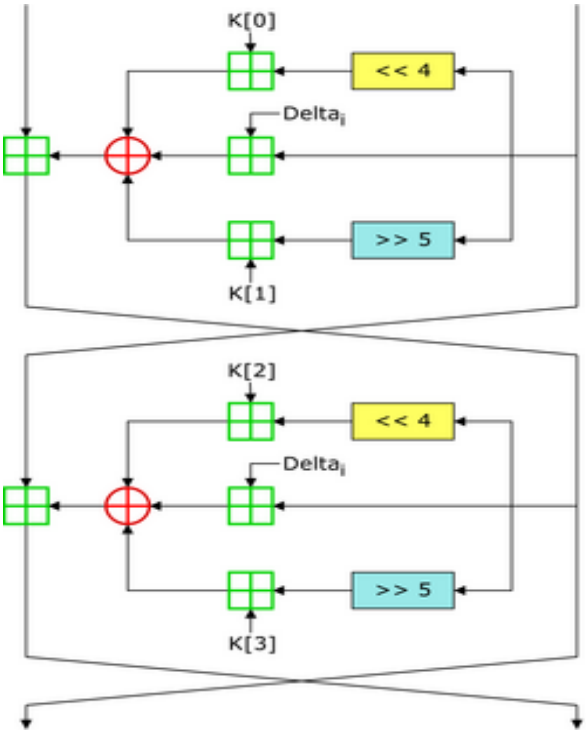


Figure 2: Computation of TEA algorithm

3.3 HiveMQ

This is a broker (MQTT) which is available for public. It helps in fast messaging and is used for reliable data transfer between the IoT devices and the systems (Figure 3).

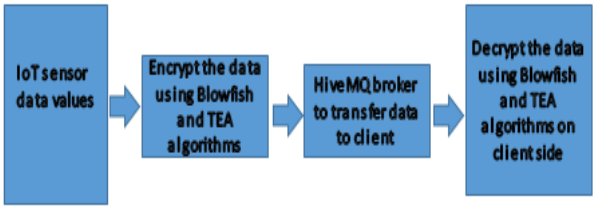
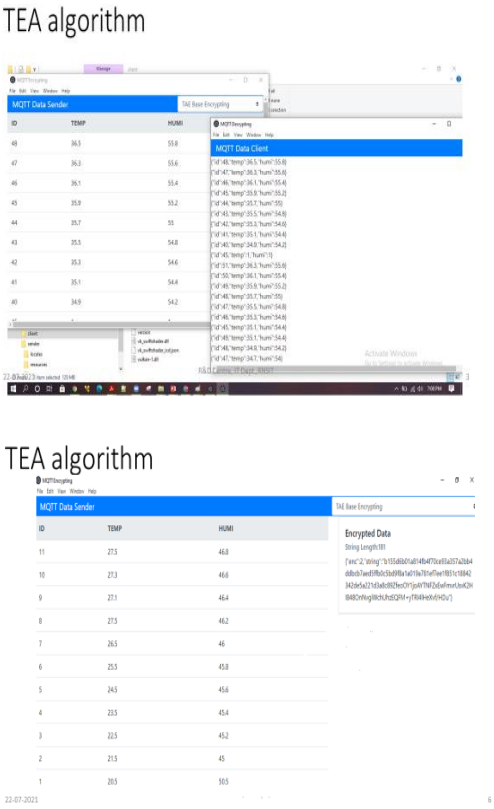
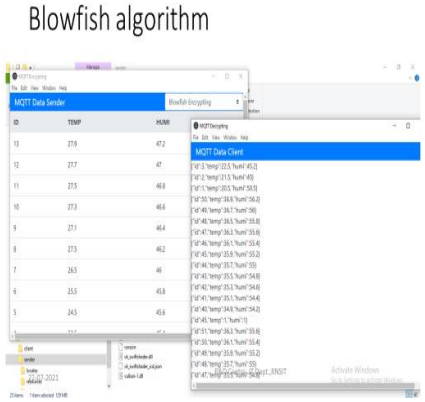


Figure 3: Block diagram of encryption and Decryption

4. Results

The encryption and decryption of the sensor data for TEA and Blowfish algorithms are shown in Figure 4.





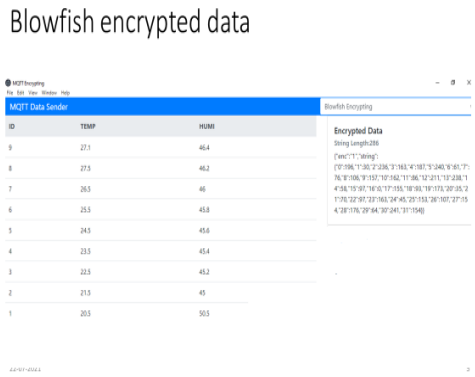


Figure 4: Encryption and Decryption results

4.1 Evaluation of the parameters using these two algorithms are shown

Parameters for comparision

Algorithm	Encryption Time	RAM Usage	CPU utilization
Blowfish	1200ms	1.5MB	0.3%
TEA	1373ms	2MB	0.27%

References

1. Palak Jain, Nikhil Kumar Singh, Deepak Singh Tomar, Defacement of Colluding Attack Using Blowfish Algorithm, International Journal of Engineering and Technology (IJET), Vol 9, No 3 Jun-Jul 2017, pp. 2420-2434.

2. Priyadarshini patil, Prashant Narayankar, Narayan D G, Meena S M, A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish, International Conference on Information Security & Privacy, pp. 11-12 Nagpur, INDIA, Science Direct, ELSEVIER, December 2015

3. Susha Surendran(NYIT, Abu Dhabi, UAE), Amira Nasef (NYIT, Abu Dhavi, UAE), Babak D. Beheshti(NYIT, Old Westbury, NewYork), A survey of Cryptograhphic Algorithms for IoT Devices, IEEE, 2018.

4. Madhumita Panda, Performance Analysis of Encryption Algorithms for Security, International conference on Signal Processing, Communication, Power and Embedded System, 2016.

5. Sahil Kataria, Kavita Singh, Tarun Kumar, Maninder Singh Nehra, ECR(Encryption with Cover Text and Reordering)based Text Steganography, IEEE Second International Conference on Image Information Processing, 2013.

6. Bharati Wukkudada, Kirti Wankhede, Ramith Nambiar, Amala Nair, Comparison with HTTP and MQTT in Internet of Things (IoT), Proceedings of the International Conference on Inventive Research in Computer Applications, IEEE, Xplore Compliant Part Number:CFP18N6/-ART;ISBN:9/8-1-5386-2456-22018,2018.