SECURE IOT IN WSN NETWORK

Dr.S.Gayathri[1], Mrs.D.Radha[2]
[1]Asst.Professor& HOD, UG & PG Dept. of Computer Science,ShriKrishnaswamy College for Women,Anna nagar, Chennai-40.
[2] Asst. Professor, UG & PG Dept. of Computer Science, ShriKrishnaswamy College for Women, Anna nagar, Chennai-40.

Abstract- IOT can be viewed as a gigantic network consisting of networks of devices and computers connected through a series of intermediate technologies like RFID's,wireless connections may act as enablers of this connectivity. The increased number of communication generates vast amount of data and the security of data can be threat. Even though IoT is secured with encryption and authentication, sensor nodes are exposed to wireless attacks inside the WSN and from the internet. Since the nodes inside the WSN can be captured and cloned, protection of data is essential. In this paper, we propose an encryption algorithm named as Secure IoT (SIT). It is a 16-bit block cipher and requires 16-bit key to encrypt the data.

Keywords: - SIT, WSN, RFID,c-Function, Encryption.

1. Introduction

The internet of things (IoT) is the network of physical objects or things embedded with electronics, software, sensors and network connectivity, which enables these objects to collect and exchange data. IoT allows objects to be sensed and controlled remotely across existing network infrastructure creating opportunities for direct integration between the physical world and the computer-based systems, thus resulting in improved efficiency and accuracy.
Many IoT devices don't encrypt messages before sending them over the network. So, to establish secured private communication, the data has to be confidential. To achieve this, an encryption algorithm named as Secure IoT (SIT) is proposed.

2. Security Challenges In Iot

IoT is extremely open to attacks for the reasons that there is a fair chance of physical attack on its components as they remain unsupervised for long time.
Secondly, due to the wireless communication medium, the eavesdropping is extremely simple. In order to handle all the issues related to security and confidentiality of data, the proposed algorithm is designed for IoT to deal with the security and resource utilization challenges.

3. Proposed Algorithm- SIT

The proposed algorithm bestows a simple structure that fits for implementing in IoTenvironment. SIT is a symmetric key block cipher that constitutes of 16-bit key and plain text. The encryption process consists of 5 rounds where each round is based on some mathematical functions that operates on 4 bits of data.

The next process is symmetric key algorithm is generation of key which involves complex mathematical operations.

Notation	Function
$\oplus$	XOR
$\odot$	XNOR
+, ‖	CONCATENATION

Table 1:Notations

4. Key Generation Process

Our proposed encryption algorithm is composed of 5 rounds, where each round requiring a separate key, thus we require 5 unique keys. To do so, we are proceeding with the key generation block. This SIT algorithm is a 16-bit cipher which means it requires 16-bit key to encrypt 16-bits of data.
Input – A 16-bit key Kc is taken as an input from the user and it serves as the input to the key generation block.
Process- (i) The 16-bit block performs substantial operations to hide the originality and it generates 5 unique keys.
(ii)These 5 unique generated keys shall be used in the encryption/decryption process, which remains blurred during the attack.

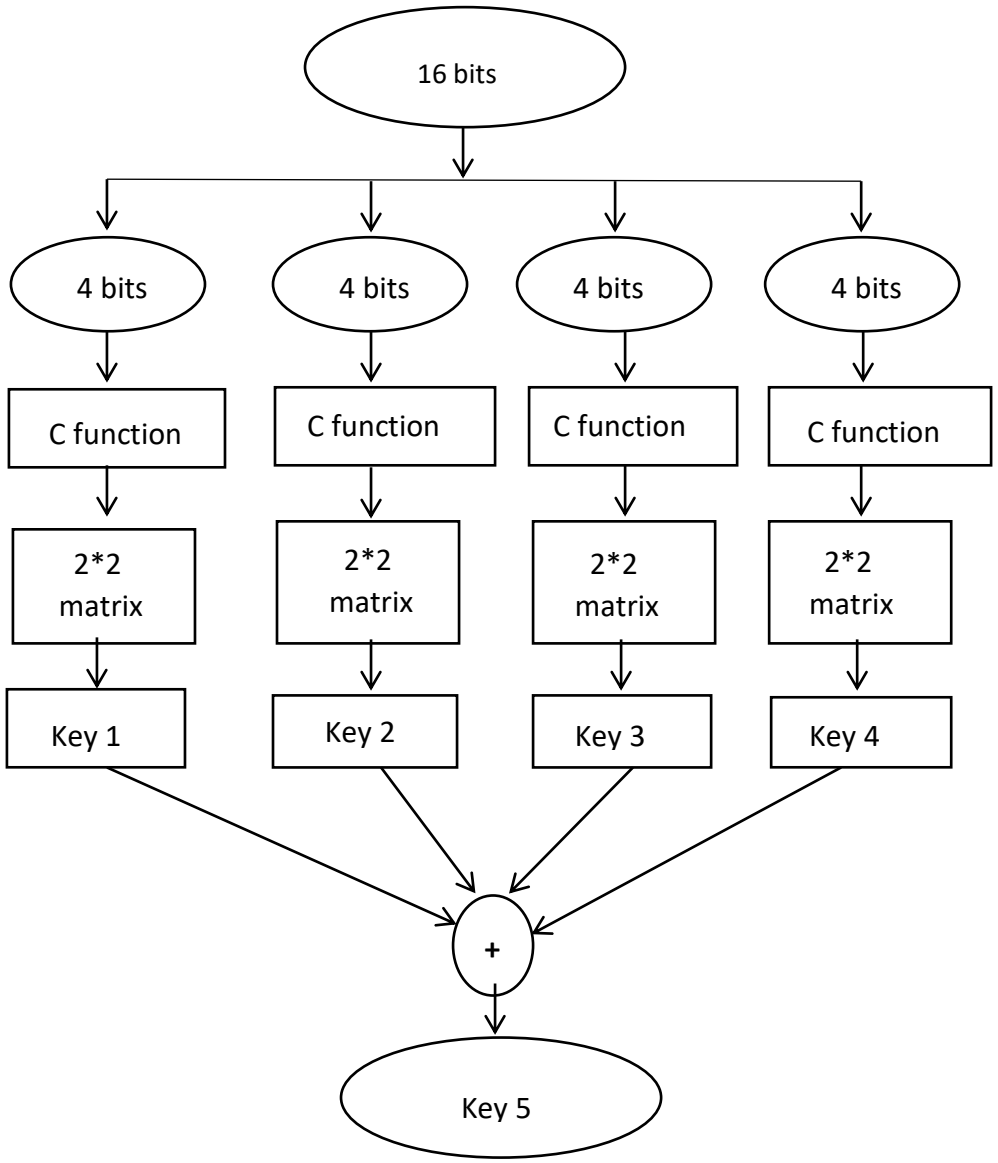
5. Components Of Key Generation

(i)The 16-bit cipher key Kc is divided into 4 segments of 4 bits each.

(ii)The c-function operates on 4-bits data. Hence, we need 4 c-function blocks. These4-bits for each c-function are obtained after the initial substitution of segments of cipher key Kc.

Explanation of f-Function

f-function is comprised of P and Q tables. These tables perform linear and non-linear transformations to hide the data.



The transformations made by P and Q tables are shown below:

Kci	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
P(Kci)	3	F	E	0	5	4	B	C	D	A	9	6	7	8	2	1

Table 1 : P TABLE

Kci	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
P(Kci)	9	E	5	6	A	2	3	C	F	0	4	D	7	B	1	8

Table 2: Q TABLE

The output of each f-function is arranged in 4 x 4 matrix as shown below:

$$Km1=\begin{pmatrix} Ka1c1 & Ka1c2 \\ Ka1c3 & Ka1c4 \end{pmatrix}$$

$$Km2=\begin{pmatrix} Ka2c1 & Ka2c2 \\ Ka2c3 & Ka2c4 \end{pmatrix}$$

$$Km3=\begin{pmatrix} Ka3c1 & Ka3c2 \\ Ka3c3 & Ka3c4 \end{pmatrix}$$

$$Km4=\begin{pmatrix} Ka4c1 & Ka4c2 \\ Ka4c3 & Ka4c4 \end{pmatrix}$$

To obtain the keys for each round, the matrices are transformed into 4 arrays of 16-bits Kr which is the round key.

K1=a1+a2+a3+a4

K2=b1+b2+b3+b4

K3=c1+c2+c3+c4

K4=d1+d2+d3+d4

To obtain the fifth key K5, an XOR operation is performed among the four round keys.

$$K5 = \bigoplus_{i=1}^{4} K_i$$

6. Encryption

The process of encryption is as follows:

(i)For the first round an array of 16-bit plain text is divided into 4 segments of 4-bits each. As the bits progresses in each round, the swapping operation is applied just to hide the data originality by altering the order of bits, essentially to create confusion in cipher text.

(ii)The round transformations are calculated by performing bitwise XNOR operations between round key Ki and Px0-4 and the same is applied between Ki and Px12-16.

(iii)The output of this XNOR operation is given as an input to the c-function.

(iv)The c-function used in encryption is same as key generation, comprised of swapping techniques.

(v)The results of final rounds are concatenated to obtain the cipher text.

$Ct = R_1 + R_2 + R_3 + R_4$

References

[1] J.Gubbi, R.Buyya, S.Marusic and M.Palaniswami,"Internet of things(iot):A vision,architectural elements, and future directions,"Future Generation Computer Systems",2013

[2]R.Want and S.Dustdar, "Activating the internet of things",2015.

[3]J.Romero-Mariona,R.Hallman,M.Kline,J.SanMiguel,M.Major and L.Kerr, "Security in the industrial internet of things",2016.

[4] H.Suo,J.Wan,C.Zou and J.Liu,"Security in the internet of things:a review",2012.

[5] D.Miorandi,S.Sicari,F.DePellegrini and I.Chlamtac, "Internet of things

(6) www.iec.ch/iecWP-internet of things.

(7) https://blog.apnic.net/2017/09/securing- iot - wireless - sensor – networks

FUTURE ENHANCEMENTS

The algorithm can be optimized in order to enhance the performance according to different hardware platforms.

The scalability of algorithm can be exploited for better security and performance by changing the number of rounds or the architecture.