International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137

Volume – 03, Issue – 04, April 2018, PP – 01-05

Implementation of High Efficient Encryption Algorithm for IoT system using Genetic Algorithm

C. Manikandan[1], V. Alamelumangai[2]

[1] *(Department of Electronics and Instrumentation Engineering, Annamalai University, India)*

[2] *(Department of Electronics and Instrumentation Engineering, Annamalai University, India)*

Abstract*:* Modern world requires controlling the industrial devices in remote manner. This would possible if and only if the present technique adopt the recent development as Internet of Things. The main limitations of the conventional techniques are that they are in lagging with security. The data from the private unit is traced by hackers or attacked by threats, which degrades the performance of the conventional networking systems. This paper proposes Genetic Algorithm (GA) based encryption and decryption algorithm in IoT server architecture in order to improve the level of security. The performance of the proposed encryption methodology in IoT server system is analyzed using Number of Changing Pixel Rate (NPCR), Unified Averaged Changed Intensity (UACI) and Information Entropy (IE).

Keywords: Internet of Things, encryption, security, Genetic Algorithm, performance.

I. Introduction

Internet of Things (IoT) is a centralized device or server which is used to capture or collect the values of the sensors in and around the world. The devices or equipments in remote can be controlled or monitored by IoT server. In this work, IoTs can be used in industrial automation and also used for many commercial applications in real time world environment. The applications of the IoT system are stated as,

- Environmental monitoring
- Energy management
- Medical and healthcare
- Building and home automation

Figure 1 IoT Interfacing with remote devices

The generic interfacing architecture of IoT is shown in Fig.1. Here, different devices such as computers, mobile phones, electric devices, cameras and vehicles are connected and controlled by IoT technology. This paper proposes an efficient methodology to improve the level of security in industrial applications. Section 2 analyzes various conventional methodologies for security concern in IoT. Section 3 proposes an efficient encryption and decryption methodology for the security concern in Industrial IoT, section 4 discusses experimental results of this proposed method. Finally, section5 depicts the conclusion of this paper.

II. Literature Survey

Ghulam Muhammad et al. (2017) provided a solution for health system monitoring using IoT. The authors analyzed the performance of their proposed system in cloud environment. This system was designed using voice mode data transfer. The authors analyzed their proposed system in terms of storage and service sharing between different networks. Mujahid Mohsiny et al. (2016) proposed a methodology to secure the

network activities using IoT technology. The authors detected potential attacks and threat attacks which were affected the system behavior through data transmission and reception. The redundancy level was reduced by implementing the systems configuration through IoT technique. The performance of this methodology was analyzed in terms of memory, network size and mean. Jarkko Kuusijarvi et al. (2016) analyzed security threats in IoT data processing. The authors proposed trusted Network Edge Device to secure the networking devices in an effective manner. Distributed Denial of Service attacks were detected and mitigated which affected the service in IoT. D. Díaz-Sánchez et al. (2016) designed store and forward proxy for improving the security level of the system using IoT technology. The authors developed a cost effective security system for Machine to Machine (M2M) networks. They also proposed asynchronous protocols to improve the level of confidentiality for security networks. Wooseong Kim et al. (2016) proposed Adaptive Resource Scheduling algorithm for improving the security level in IoT technology. The authors analyzed the security performance in heterogeneous cellular IoT network architecture.

Chakib Bekara et al. (2014) proposed smart grid security using IoT technology. The authors analyzed the security issues and challenges in conventional security networks. The electric and information flow of this proposed algorithm was analyzed. Attlee M. Gamundani et al. (2014) used Augmented Approach Model for algorithmic design to improve the level of security in IoT networks. The authors analyzed its performance in different network domains.

The following points are observed from the conventional methods as stated below.

- The security level of the conventional IoT system is not optimized.
- The conventional methods were not suitable for larger set of nodes or sensors.
- The memory utilization of the conventional IoT system is high due to its higher latency.

This paper proposes an efficient encryption algorithm for improving the security level of the IoT system using GA technique to overcome the limitations of the conventional methodologies.

III. Proposed Methodology

The proposed IoT security system using GA based encryption scheme is shown in Fig. 2. This proposed system consists of key generator module, GA modules and XOR operation module. Key generator module is responsible for generating the security key for encrypting and decrypting the packets from sensor units.

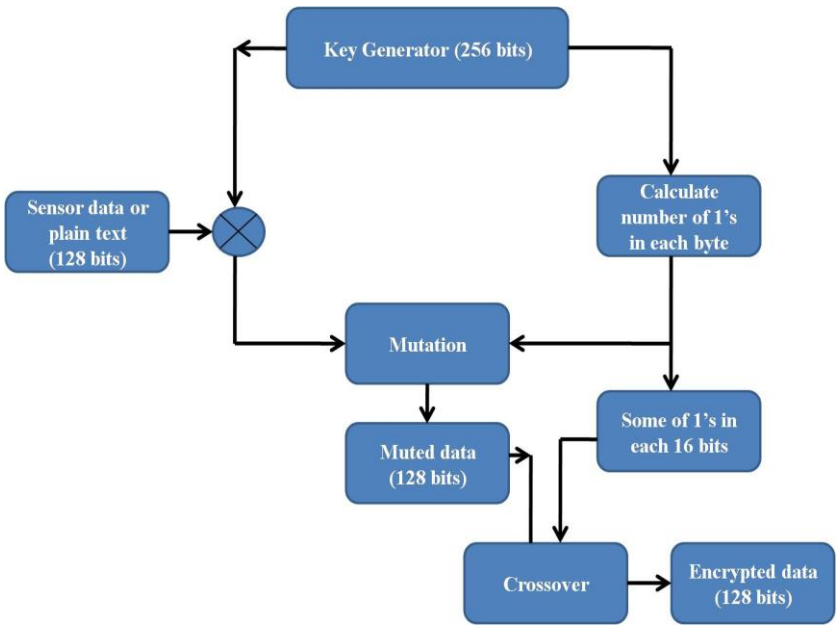

Figure 2 Proposed flow of Encryption methodology

The proposed encryption algorithm is explained in the following section. The data received from sensor unit in industry is considered as packets. The length of the packet is 128 bits long and it is also known as plain text. The architecture of key generator unit is shown in Fig.3. This key generator unit is used to generate keys which is used for encrypting the data from sensor units. Mutation is the process of changing the bit position in same text. Mutation process can be categorized into either single point or multi point. In this paper, single point

mutation is used for mutation purpose. Crossover is the process of changing the bit position in between two data. Cross over process can be categorized into either single or multi point. In this paper, single point cross over is used for cross over purpose.

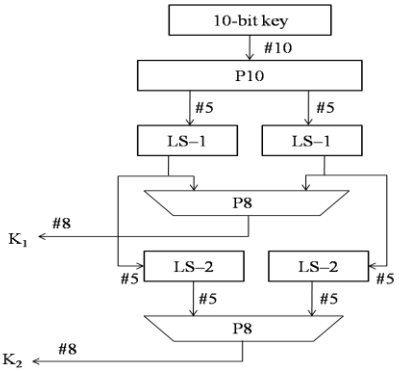

Figure 3 Key Generator Module

Initially, the 10 bit key is permuted using P10 permutation box and these permuted 10 bit key is splitted into two adjacent five bits. These individual five bits are now passed through left shift by one module inorder to produce left shifted data. The output from Left shift module are applied to permutation box 8 which produces first 8-bit key and then each individual output from LS1 unit is now shifted one bit left inorder to produce another two individual five bits. These left shifted bits are now applied to permutation box 8, which produces next 8-bit key. Hence, this 10 bit key produces 16 bit key for each iteration. In this manner, it produces 256 bit key.

The following steps are used for encrypting the packets which are received from sensor units, as described below.

Step 1: Perform XOR operation between 128-bit plain text and first 128 bits of secret key.

Step 2: Compute number of ones in each byte of last 128 bits of secret key.

Step 3: Perform mutation between 128 bit XOR-ed data with number of ones in last 128-bit secret key.

Step 4: Perform crossover between 128-bit muted data and sum of ones in each 16 bits, which produces 128 bit cipher data.

The decryption process is the reverse process of encryption which is carried out in the receiver side of IoT server.

IV. Results and Discussion

The performance of the proposed encryption methodology in IoT server system is analyzed using the following parameters as stated below.

- Number of Changing Pixel Rate (NPCR).
- Unified Averaged Changed Intensity (UACI).
- Information Entropy.

The security of the proposed encryption methodology is analyzed using the performance evaluation parameters NPCR and UACI.

NPCR

The performance of the decoded information in receiver IoT system is evaluated interms of NPCR and it ranges between 0 and 100. The performance of the proposed encryption system is high when it has higher value of NPCR and the performance of the proposed encryption system is low when it has lower value of NPCR.

It is represented as,

$$NPCR = \frac{1}{X*Y}\sum K(i,j) \quad (1)$$

In this expression, the transmitted and received data length is represented by X and Y, respectively. Let $K1(i,j)$ is the sensed and transmitted data and $K2(i,j)$ is the received data.

$$k(i,j) = \begin{cases} 1, & if \;\; k1(i,j) == k2(i,j) \\ 0, & else \end{cases} \quad (2)$$

UACI

The performance of the decoded information in receiver IoT system is evaluated interms of UACI and it ranges between 0 and 100. The performance of the proposed encryption system is high when it has low value of UACI and the performance of the proposed encryption system is low when it has high value of UACI.

$$UACI = \frac{1}{X*Y}\sum_{0}^{m-1}|k1(i,j) - k2(i,j)|$$

Where as, the total number of sensors in experiment is represented as 'm'.

Information Entropy (IE)

The encryption level of the proposed system is determined by measuring the information entropy of the received data. The value of information entropy lies between 0 and 15. The security of the proposed system is high when the value of information entropy is greater than or equals to 8. The expression for computing information entropy of the proposed system is given as,

$$EN = \sum_{i=1}^{t} p(mi) * log2[1/p(mi)] \quad (3)$$

Where, p(mi) : The probability of the symbol mi and t : Total number of symbols.

Table 1 Performance analysis of proposed system interms of NPCR

Number of sensors	NPCR (%)
10	98.29
20	97.37
30	96.35
40	93.64
50	92.84
60	91.57
70	90.63
Average	94.38

Table 1 shows performance of the proposed security methodology IoT server interms of NPCR. The proposed system has 98.29% of NPCR when 10 numbers of sensor nodes in IoT system and the proposed system has 90.63% of NPCR when 70 number of sensor nodes in IoT system. The average NPCR for the proposed system is 94.38%.

Table 2 Performance analysis of proposed system interms of UACI

Number of sensors	UACI (%)
10	10.27
20	12.64
30	14.85
40	16.84
50	17.56
60	18.05
70	19.56
Average	15.68

Table 2 shows performance of the proposed security methodology IoT server interms of UACI. The proposed system has 10.27% of UACI when 10 numbers of sensor nodes in IoT system and the proposed system has 19.56% of UACI when 70 number of sensor nodes in IoT system. The average NPCR for the proposed system is 15.68%.

Table 3 Performance analysis of proposed system interms of IE

Number of sensors	IE (%)
10	12.38
20	11.29
30	10.06
40	9.87
50	9.81
60	8.76
70	8.01
Average	10.02

Table 3 shows performance of the proposed security methodology IoT server interms of IE. The proposed system has 12.38% of IE when 10 numbers of sensor nodes in IoT system and the proposed system has 8.01% of UACI when 70 number of sensor nodes in IoT system. The average NPCR for the proposed system is 10.02%.

Table 4 Performance Comparisons

Number of sensors	**Conventional Method (H. Ko et al. 2016)**		**Proposed Method**	
	NPCR (%)	**UACI (%)**	**NPCR (%)**	**UACI (%)**
10	92.75	16.76	98.29	10.27
20	91.46	18.56	97.37	12.64
30	90.86	19.59	96.35	14.85
40	89.65	21.85	93.64	16.84
50	87.45	28.89	92.84	17.56
60	86.75	29.46	91.57	18.05
70	85.45	31.96	90.63	19.56
Average	**89.19**	**23.86**	**94.38**	**15.68**

The performance comparisons of the proposed system with conventional methodology are shown in Table 4, interms of NPCR and UACI. The conventional system achieved 89.19% of average NPCR while the proposed system achieves 94.38% of NPCR. The performance of the proposed system achieves 5.49% of improvement in NPCR when compared with conventional system. The conventional system achieved 23.86% of average UACI while the proposed system achieves 15.68% of UACI. The performance of the proposed system achieves 34.28% of improvement in UACI when compared with conventional system.

V. Conclusions

This paper proposes an efficient encryption and decryption algorithm for the protection of data from hackers or attackers in IoT server. This proposed algorithm is based Genetic Algorithm which constitues mutation and crossover. The key which is generated by this encryption algorithm is used to fuse the secured key with sensed data in IoT server. This encrypted data are transferred to the remote unit in a secured way. The security of the proposed encryption methodology is analyzed using the performance evaluation parameters NPCR and UACI.

References

[1]. Ghulam Muhammad, SK Md Mizanur Rahman, Abdulhameed Alelaiwi, and Atif Alamri, Smart Health Solution Integrating IoT and Cloud: A Case Study of Voice Pathology Monitoring, *IEEE Communications Magazine* , January 2017.

[2]. D. Díaz-Sánchez, R. S. Sherratt, F. Almenarez, P. Arias and A. Marín, Secure store and forward proxy for dynamic IoT applications over M2M networks, IEEE Transactions on Consumer Electronics, 62(4), 389-397.

[3]. Wooseong Kim, Adaptive Resource Scheduling for Dual Connectivity in Heterogeneous IoT Cellular Networks,*International Journal of Distributed Sensor Networks*, 12(4).

[4]. Chakib Bekara,Security Issues and Challenges for the IoT-based Smart Grid, *Procedia Computer Science* ,34, 532-537.

[5]. Attlee M. Gamundani, An Algorithmic Framework Security Model for Internet of Things. *International Journal of Computer Trends and Technology (IJCTT*) ,12(1),16-20.

[6]. H. Ko, J. Jin and S. L. Keoh, Secure Service Virtualization in IoT by Dynamic Service Dependency Verification, *IEEE Internet of Things Journal*,3(6), 1006-1014.

