Performance Analysis of Trusted Industrial Networks using Internet of Things

C.Manikandan[1], V. Alamelumangai[2]
[1]Research Scholar,[2]Professor
[1,2]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 an efficient encryption methodology on the industrial sensed data in order to protect them from various kinds of attacks or threats. This proposed algorithm is based on Affine-Projective transformation and the performance of the proposed encryption algorithm based IoT system is analyzed in terms of Packet Delivery Ratio (PDR), delay and data overhead.

Keywords: Encryption, Internet of things, sensors, performance, attacks

1.INTRODUCTION

Today, the usages of internet are high due to the development of technology. The distant devices or units are controlled by a single device through internet. Monitoring and controlling of different numerous devices through internet is called as Internet-of-Things (IoT). This IoT technique can be used in different scenario like home applications, industrial need and military usage. In case of home applications, all the devices used in user home can be continuously monitored and controlled by remote unit through the development of IoT technology between devices. In case of industrial applications, the machines are controlled and monitored by remote unit, through which the accidents in an unmanned area can be avoided. Gartner, Inc estimated the level of growth for the device usage in IoT was 20.8 billion devices in 2020 year. The multimedia data from various service providers are stored in large cloud area. Hence, there must be the high level of data confidentiality in handling these data services between different networks or service providers.

Figure 1 Architecture of IoT

The generic 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 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.

2. 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 algorithm for improving the security level of the IoT system using Hierarchical-clustering technique to overcome the limitations of the conventional methodologies.

3.PROPOSED METHODOLOGY

In this paper, Linear Projective Encryption (LPE) is proposed to encrypt the sensed information which is sent by different sensors in chemical industry. This proposed LPE algorithm is based on Affine-Projective transformation. The encryption algorithm is divided into two sections as linear mode and Non-Linear mode. The mode is selected based on the last bit in the received signal. The mode is set to linear mode if the last bit is low and the mode is set to non-linear mode if the last bit is high.

Algorithm 1

Mode: Linear mode

Input variables: X1,Z1,X2 and Z2
Output variables:

Step 1: Initial set up of variables are done as stated below:
- X1=1; Z1=0;
- X2=xp; Z2=1;

Step 2: Swapping of input variable to static variable
- Let T=Z2;

Step 3: Compute the discriminate points (Z2 and X2) using the following equations as,
- Z2=(X1*Z2+X2*Z1)^2;
- X2=xp*Z2+X1*X2*T*Z1;

Step 4: Swapping of input variable to static variable and determine the looping parameters as,
- T=X1;
- X1=X1^4+b*Z1^4;
- Z1=T^2*Z1^2

Algorithm 2

Mode: Non-linear mode

Input variables:
Output variables:

Step 1: Initial set up of variables are done as stated below:
- X1=1; Z1=0;
- X2=xp; Z2=1;

Step 2: Swapping of input variable to static variable

- Let T=Z1;

Step 3: Compute the discriminate points (Z2 and X2) using the following equations as,

- Z1=(X1*Z2+X2*Z1)^2;
- X1=xp*Z1+X1*X2*T*Z2;

Step 4: Swapping of input variable to static variable and determine the looping parameters as,

- T=X2;
- Z2=T^2*Z2^2;

Algorithm 1 explains the concept of the LPE in linear mode and Algorithm 2 explains the concept of the LPE in non-linear mode. The linear and non-linear mode is selected based on the last bit in the received signal packet from sensor nodes. The output of the linear or non-linear mode of LPE algorithm is assigned to the variable 'KEY', which is used for encrypting the sensed information.

The encryption is applied on sensed data using the generated KEY. All sensed data are XOR with generated KEY in the server of IoT. This encrypted information's are passed to the remote unit.

4.RESULTS AND DISCUSSION

In this paper, 4 sensors with different quantity as temperature, humidity, proximity sensor and thermal Anemometry are used to measure the industrial parameters in chemical industry. Temperature and humidity sensors are used to measure the temperature and humidity of the machines used in chemical industry. Proximity sensor is used to detect the presence or absence of an object in restricted areas. It is also used for jam detection in complex machinery systems. Thermal Anemometry sensor is used to monitor the velocity in gas flows. In this experimentation, 12 temperature and humidity sensors, 20 proximity sensors and 30 thermal Anemometry are used. The total number of sensors used in this paper is 74 sensors. All these sensors placed in chemical industry are controlled by remote unit through internet which incorporated IoT technology.

The remote unit and inbuilt unit in industry use a novel encryption algorithm to protect the data from UN-authorized users. Both units are incorporated with encryption and decryption algorithm. The remote unit asks keyword which is generated by the proposed encryption algorithm and matches with dataset keyword. If both are identical, then it allows accessing the sensors available in chemical industry. All data captured by sensor units at chemical industry are transferred to the remote unit through internet. The IoT server encrypts these data with the secured key and transferred to the remote unit via internet. The remote unit receives these data and decrypt using the same key which is generated by IoT server. Then, the performance of the proposed system is measured in terms of Packet Delivery Ratio (PDR).

Table 1 Analysis of PDR

Number of sensors	PDR (%)
10	97.28
20	95.27
30	93.84
40	92.64
50	91.07
60	89.36
70	87.94
Average	**92.48**

The proposed system achieves 92.48% of PDR for total number of 70 sensors as depicted in Table 1. The performance of the PDR is decreased when increasing the number of sensors used in chemical industry. High PDR is achieved at low number of sensors and low PDR is achieved at high number of sensors.

Table 2 Analysis of Delay

Number of sensors	Delay (ms)
10	20.37
20	26.91
30	28.61
40	30.27
50	32.19
60	33.29

70	35.71
Average	**29.62**

The proposed system achieves 29.62 ms of average delay for total number of 70 sensors as depicted in Table 2. The performance of the proposed system in terms of delay is increased when increasing the number of sensors used in chemical industry. High delay is achieved at high number of sensors and low delay is achieved at low number of sensors.

Table 3 Analysis of data overhead

Number of sensors	Data overhead (Kb)
10	11.28
20	13.29
30	15.86
40	16.96
50	18.56
60	22.18
70	24.75
Average	**17.55**

The proposed system achieves 17.55 Kb of average data overhead for total number of 70 sensors as depicted in Table 3. The performance of the proposed system in terms of data overhead is increased when increasing the number of sensors used in chemical industry. High data overhead is achieved at high number of sensors and low data overhead is achieved at low number of sensors.

Table 4 Performance Comparisons

Number of sensors	Conventional Method (H. Ko et al. 2016)		Proposed Method	
	Delay (ms)	Data overhead (Kb)	Delay (ms)	Data overhead (Kb)
10	20.37	11.28	26.4	11.03
20	26.91	13.29	46.6	21.13
30	28.61	15.86	69.7	30.60
40	30.27	16.96	91.5	41.34
50	32.19	18.56	113.0	51.43
60	33.29	22.18	156.9	61.53
70	35.71	24.75	175.1	71.64
Average	**29.62**	**17.55**	**97.02**	**41.24**

Table 4 shows the comparisons of the proposed methodology with respect to conventional methodology in terms of delay and data overhead.

5 CONCLUSIONS

This paper proposes an efficient algorithm for the protection of data from hackers or attackers in IoT server. This algorithm is based on affine and projective transformation. 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 an secured way. The performance of the proposed methodology is analyzed in terms of packet delivery ratio, delay and data overhead. The proposed system achieves 92.48% of PDR, 29.62 ms of average delay and also achieves 17.55 Kb of average data overhead for different set of sensors in industrial environment.

References

1. Mujahid Mohsiny, Zahid Anwary, Ghaith Husariy, Ehab Al-Shaery, Mohammad Ashiqur Rahman, “IoTSAT: A Formal Framework for Security Analysis of the Internet of Things (IoT)”, 2016 IEEE Conference on Communications and Network Security (CNS).
2. Jarkko Kuusijarvi, Reijo Savola, Pekka Savolainen, Antti Evesti, “Mitigating loT Security Threats with a Trusted Network Element”, The 11th International Conference for Internet Technology and Secured Transactions (ICITST-2016).
3. 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.

4. 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," in IEEE Transactions on Consumer Electronics, vol. 62, no. 4, pp. 389-397, November 2016.
5. Wooseong Kim, "Adaptive Resource Scheduling for Dual Connectivity in Heterogeneous IoT Cellular Networks", International Journal of Distributed Sensor Networks, Vol 12, Issue 4, 2016.
6. Chakib Bekara, "Security Issues and Challenges for the IoT-based Smart Grid", Procedia Computer Science Volume 34, 2014, Pages 532-537.
7. Attlee M. Gamundani, "An Algorithmic Framework Security Model for Internet of Things". International Journal of Computer Trends and Technology (IJCTT) V12(1):16-20, June 2014.
8. H. Ko, J. Jin and S. L. Keoh, "Secure Service Virtualization in IoT by Dynamic Service Dependency Verification," in IEEE Internet of Things Journal, vol. 3, no. 6, pp. 1006-1014, Dec. 2016.