Asian Journal of Computer Science and Technology
ISSN: 2249-0701 Vol.7 No.2, 2018, pp.52-56

ARO_EDGE: A Technique to Ensure Data Security in Internet of Things (IoT)

A. Vithya Vijayalakshmi[1] and L. Arockiam[2]
[1]Ph.D. Scholar, [2]Associate Professor,
[1,2]Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India
E-Mail: vithyanbalagan@gmail.com

Abstract **- Recently, e-health care, smart home, smart city, smart car and smart car services have been receiving attention all over the world. In smart health care, there are many sensors are communicating between each other and connected to the global network connection. Therefore, there is a problem in securing the data sensed from the various medical IoT devices. Lightweight and efficient way of providing secure communication in the IoT are the need of the hour. To overcome this problem, a technique has been proposed. This paper proposes a confidentiality technique, named ARO_EDGE to secure the data in IoT devices. This proposed confidentiality technique is based on data obfuscation technique to prevent the data from the attackers and unauthorized users.**
Keywords: **Internet of Things, Smart Healthcare, Data Security, Obfuscation Technique**

I. INTRODUCTION

Internet of Things (IoT) provides a platform to connect anything from anyplace and anytime. It aims to integrate physical objects, peoples, computing systems over a common network to interact and communicate between each other. There is a vast increase in number of users, services and applications in IoT. The expected volume of connected devices require the use of machine-to-machine communication meaning that humans will no longer have direct control over with whom or what our devices are communicating [1]. There are many applications available in IoT such as E-Health, Retail & Logistics, Smart Transportation, Smart Environment, Smart Home, Energy Conservation, Environmental Monitoring etc [2]. In IoT, many types of sensors, smart devices and RFID tags collect data depending on their purpose, some of the data might be highly sensitive such as data collected from smart healthcare devices and smart home devices. These calls for the security on the device which must be secure the collected data and send it to the common gateway/server.

To overcome the security issues, IoT needs identity authentication mechanisms and protection of the confidentiality of the data. Data confidentiality, integrity and availability are the three basic areas of security. The main objective of data confidentiality is protecting the privacy of sensitive information by using some mechanisms and avoiding the unauthorized access. For IoT devices, data confidentiality means the data collected by the sensors should not be transmitted to an unauthorized user. Data encryption is a mechanism to ensure the data confidentiality. Where, the encrypted data convert into cipher text and unauthorized users cannot easily access the data. In the IoT system, the data is encrypted in the Wireless Sensor Network (WSN) nodes and transmitting to the gateway.

In this paper, a cryptographic algorithm to enhance the data security at the device level is proposed. This algorithm deals with the data security based on cryptographic techniques. The proposed algorithm, however, is mainly focused on data collected from the IoT sensors / devices. T he requirements of developing a new cryptographic algorithm are strong security mechanism (encryption/decryption) with low power. The main reason for developing a new cryptographic algorithm is to enhance the efficiency of end-to-end communications in low resources smart devices.

II. RELATED WORKS

Saurabh Singh *et al.* [3] discussed various lightweight cryptographic algorithms such as lightweight stream ciphers block ciphers and hash function. Based on block size, key size, number of rounds, and structures they analysed the cryptographic algorithms. They focused on research security issues and challenges and discussed the security architecture in IoT for constrained device environment. They proposed Hybrid Lightweight Algorithm (HLA) and explained with a service scenario of a smart home for an improvement of resource constrained IoT environment. The proposed HLA is a combination of lightweight symmetric algorithm and lightweight asymmetric algorithm to minimize computation time, consume less power, fast efficient and assures all the possible security. The HLA scheme provides two encryption schemes based on the analysis of device parameters such as data size, memory space, computation power, and battery power. Based on the parameters the lightweight algorithms are applied to the smart devices.

Lobna Yehia *et al.* [4] discussed the security for healthcare systems mainly focusing on the data security. They proposed a hybrid security technique for internet of things healthcare applications. Here, they combined symmetric encryption and asymmetric encryption to secure the healthcare data. They also showed that the hybrid algorithms use the maximum security to the data. Amirhossein Safi [5] proposed a hybrid encryption with the combination of AES and NTRU algorithm to enhance computational speed and to reduce computational complexity. By implementing they proved that this type of encryption generates strong security and low computation.

Salvador Perez *et al.* [6] introduced an encryption scheme based on the lightness of symmetric cryptography, and the use of attribute-based encryption. To secure the data, the proposed encryption scheme combines the lightness and effectiveness of symmetric key cryptography with Ciphertext-Policy Attribute-Based Encryption scheme (CPABE). The combination of Symmetric and CP-ABE was named as SymCpAb. The data are encrypted by using the AES algorithm with symmetric keys and the keys are secured by using CP-ABE scheme. This helps the users to avoid data leakage from unauthorized access. Zhen-Yu Hong *et al.* [7] proposed a new concept of fusion encryption algorithm, which is a combination of DES and RC4 algorithm. The proposed algorithm used to encrypt the transmitted data. The simulation result shows that this fusion encryption improves the difficulty of breaking the cipher text and decreases the cost.

III. PROBLEM DEFINITION

In IoT, everything is connected and communicated with each other which generate large volumes of data. The user wants the data to be secured while storing, accessing and processing and their data through devices. Data confidentiality is essential in Internet of Things. It is the ability to hide messages from an attacker so that any message communicated via the sensor remains confidential. This is the most important issue in data security. A sensor node should not disclose its data to the neighbours. Thus, to make sure that the client devices are secured for easy access & usage. The data security in internet of things devices is needs to be addressed.

IV. PROPOSED TECHNIQUE

In this technique, a concept of storing sensitive data using data obfuscation is introduced. To ensure the data confidentiality, the data are encrypted using obfuscation technique before sending the data to the local server / gateway. This is symmetric key encryption technique. In terms of existing techniques, symmetric encryption is suitable for embedded devices, which are important building blocks of IoT. Unlike, asymmetric encryption which usually requires difficult mathematical operations such as modular exponentiation of large integers and complex manipulations on elliptic curves, symmetric encryption is effective in devices with limited resources. The scope of this research work is to encrypt the numerical sensor data sensed from the medical IoT devices. The proposed technique is a new symmetric encryption technique that allows the encryption to be performed securely in IoT devices, considering the following constraints for IoT devices: (i) Memory of the devices (ii) Power of the devices and (iii) size of the devices etc.

Data obfuscation is aimed to convert IoT data into unintelligible or confusing data. By using this technique, the data is purposely scrambled to prevent from unauthorized access. Data obfuscation techniques are used to prevent the intrusion of sensitive IoT data. Types of data obfuscation are: Storage, Aggregation, Ordering and Encoding. Encoding uses mathematical functions to obfuscate the data. This technique uses sqrt(), pow(), mod(), functions for obfuscation and for de-obfuscation of the IoT data.

A. Procedure for Obfuscation

Step 1: Count the number of values in the plain text (plain text =numerical value)
Step 2: Sum the plain text with the key values generated
Step 3: Key is a set of single digit prime values starting from 2 and goes on.
Step 4: The numeric value is split into digits
Step 5: Calculate the square of each digits and append
Step 6: Interweave the square of the digits
Step 7: Find Modulus of the interweaved value by using the key

B. Procedure for De-obfuscation

Step 1: Multiply the secret key value with the key and sum with the cipher text value
Step 2: Interweave the digits of the ciphertext
Step 3: Find the square root of the interweaved values
Step 4: Subtract the square root values with the key generated
Step 5: The subtracted value will be the plain text

V. APPLICATION

In 2020, it is expected that the number of Internet-connected devices will be more than 50 billion [8]. There are many IoT applications, and within those, smart healthcare system is one of the biggest challenges that our society faces now-a-days. The main components of the Smart Healthcare system include telemedicine, electronic health records, communication protocol among the components of the system [9]. IoT has many advantages in the field of smart healthcare by using smart sensors, equipment, detectors, etc. For example, the temperature, Blood Pressure and Heart rate of patients can be measured by temperature sensor, Heart rate sensor etc. [10]. This kind of sensitive data should be secured and protected. The data captured by a set of sensors can be collected, processed and secured before transmitting it into other devices. The proposed technique is used to secure the numerical healthcare data collected from the sensor/IoT medical devices.

TABLE I OBFUSCATION AND DE-OBFUSCATION TECHNIQUE

Pseudo code of proposed ARO_EDGE Obfuscation technique	Pseudo code of proposed ARO_EDGE De-obfuscation technique
• Start • PT ← plaintext • N ← length(PT) *//Generate a Key value and store it in PV(i)* • for i ← 0 to N-1 • TV(i) ← PT(i) + PV(i) *//Count the digits in TV(i) and split into digits (D)* • Count = D(i) • SV(i) ← SQRT (D(i)) *// Append the single digit value with ‘0’* *//Interweave the square of the digits* • WV(i) ← interweave(SV(i)) *//Find the module value MOD for WV using PV(i)* • MV(i) ← WV(i)%PV(i) • SK(i) ← WV(i)/PV(i) • CT(i) ← MV(i) • end for • end	• Start • CT← Cipher text *// Count the values in cipher text* • N ← count (CT(i)) • for i ← 0 to N-1 *//Multiply the secret key value with the key generated and sum with the cipher text value* • MUL(i) ← SK(i)*PT(i) + CT(i) *//Interweave the square of the digits* • WV(i) ← interweave(MUL(i)) *//find the square root* • ST(i) ← SQRT(WV(i)) *//Subtract the value with the key generated* • PT(i) ← SUB(ST(i)) • Plaintext ← PT(i) • end for • end

VI. ARO_EDGE OBFUSCATION PROCEDURE WITH SAMPLE DATA

Consider the following values for obfuscation

25 37 42 15 57

Step 1: Count the number of values (N) in Plain Text (PT)

Step 2: The plain text values are

PT(i)	Value
PT(0)	25
PT(1)	37
PT(2)	42
PT(3)	15
PT(4)	57

Step 3: Generate key value. Key – single digit prime value PV(i). Starting from 2 and goes on.. Key – 2, 3, 5, 7

PV(i)	Value	Key
PV(0)	25	2
PV(1)	37	3
PV(2)	42	5
PV(3)	15	7
PV(4)	57	2

Step 4: Sum the key value with the plain text

TV(i)	Value
TV(0)	27
TV(1)	40
TV(2)	47
TV(3)	22
TV(4)	59

Step 5: Calculate the square for each digit of the value and append the value with ‘0’

SV(i)	Value
SV(0)	04 49
SV(1)	16 00
SV(2)	16 49
SV(3)	04 04
SV(4)	25 81

Step 6: Interweave the square digits SV(i)

WV(i)	Value
WV(0)	0449
WV(1)	1060
WV(2)	1469
WV(3)	0044
WV(4)	2851

Find the secret key value SK(i) = WV(i) / PV(i)

SK(i)	Value
SK(0)	224.5
SK(1)	353.3
SK(2)	293.8
SK(3)	6.2
SK(4)	1425.5

Step 7: MV(i) = Modulus of WV(i) by using the key PV(i)
MV(i) = Cipher Text (CT(i))

MV(i)	Value	CT(i)
MV(0)	1	CT(0)
MV(1)	1	CT(1)
MV(2)	4	CT(2)
MV(3)	2	CT(3)
MV(4)	1	CT(4)

VII. ARO_EDGE DE-OBFUSCATION PROCEDURE WITH SAMPLE DATA

Step 1: Multiply the secret key value with the key generated and sum with the cipher text value

CT(i)	Value
CT(0)	1
CT(1)	1
CT(2)	4
CT(3)	2
CT(4)	1

MUL(i) ← SK(i)*PT(i) + CT(i)

MUL(i)	Value
MUL(0)	0449
MUL (1)	1060
MUL (2)	1469
MUL (3)	0044
MUL (4)	2851

Step 2: Interweave the digits of the ciphertext
WV(i) ← interweave(MUL(i))

WV(i)	Value
WV(0)	04 49
WV(1)	16 00
WV(2)	16 49
WV(3)	04 04
WV(4)	25 81

Step 3: Find the square root of the interweaved values
ST(i) ← SQRT(WV(i))

ST(i)	Value
ST(0)	27
ST (1)	40
ST (2)	47
ST (3)	22
SV(4)	59

Step 4: Subtract the square root values with the key generated PT(i) ← SUB(ST(i))

PT(i)	Value	Key
PT(0)	25	2
PT(1)	37	3
PT(2)	42	5
PT(3)	15	7
PT(4)	57	2

Step 5: The subtracted value will be the plain text
Plaintext ← PT(i)

25 37 42 15 57

VIII. CONCLUSION

This paper has proposed a technique to ensure data security in internet of things based on data obfuscation technique namely ARO_EDGE. According to the proposed technique, the data are obfuscated before they are communicated among devices or local gateway. This technique obfuscates numerical values of the sensor data collected from the healthcare IoT devices. It uses different mathematical function to operate the original text into unintelligible text. The proposed technique reduces the size of the plaintext and ensures the confidentiality of the sensor data at the edge level.

ACKNOWLEDGEMENT

This research was supported by a g rant from University Grants Commission (UGC) awarded to A. Vithya Vijayalakshmi under Senior Research Fellowship.

REFERENCES

[1] Maire O'Neill, "Insecurity by Design: Today's IoT Device Security Problem", Elsevier, 2016, Vol. 2, Iss. 1, pp. 48 & 49.
[2] A.Vithya Vijayalakshmi and Dr. L. Arockiam, "A Study on Security Issues and Challenges in IoT", International Journal of Engineering Sciences & Management Research, 2016, ISSN 2349-6193, Vol. 3, Iss. 11, pp. 1-9.
[3] Saurabh Sing and Pradip Sharma, Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions", Journal of Ambient Intelligence and Humanized Computing, 2017, Springer, pp. 1-18, DOI: 10.1007/s12652-017-0494-4.
[4] Lobna Yehia, Ayman Khedr and Ashraf Darwish, "Hybrid Security Techniques for Internet of Things Healthcare Applications", Advances in Internet of Things, 2015, Vol. 5, pp. 21-25.
[5] Amirhossein Safi, "Improving the Security of Internet of Things using Encryption Algorithms", International Journal of Computer and Information Engineering, 2017, Vol. 11, No. 5, pp. 540-543.
[6] Salvador Perez, Jose, Hernández-ramos, Sara N. Matheu-garcía, Domenico Rotondi, Antonio F. Skarmeta, Leonardo Straniero, and Diego Pedone, "A lightweight and flexible encryption scheme to protect sensitive data in Smart Building scenarios", IEEE, 2016, Vol. 4, pp. 8956 – 8977, DOI: 10.1109/ACCESS.2017.2695525.
[7] Zhen-Yu Hong, Zhong-Pan Qiu, Si-Liang Zeng, Shui-De Wang and Mukase Sandrine, "Research on Fusion Encryption Algorithm for Internet of Things Monitoring Equipment", IEEE, International

Conference on Frontier of Computer Science and Technology, 2017, ISSN: 2375-527X, pp. 425-429.

[8] Vermesan, O. and Friess, P. "Internet of Things Applications - From Research and Innovation to Market Deployment", 2014 (River Publishers Series in Communications).

[9] Kashif Saleem, Abdelouahid Derhab, Jalal Al-Muhtadi and Basit Shahzad, "Human-oriented design of secure Machine-to-Machine communication system for e-Healthcare society", Elsevier, Computers in Human Behavior, 2014, Vol. 54, pp. 977-985.

[10] Dharmendra Singh Rajput and Rakesh Gour, "An IoT Framework for Healthcare Monitoring Systems", International Journal of Computer Science and Information Security, 2016, ISSN 1947-5500. Vol. 14 No. 5, pp. 1-5.