International Journal of Engineering & Technology, 7 (3.34) (2018) 241-244

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Lightweight Trust Scheme for Iot

[1]Dr. S. Chithra, [2]Dr. N. Bhalaji, [3]S. Nandini

Department of Information Technology, Sri Sivasubramaniya Nadar College of Engineering, Chennai
**Corresponding author E-mail: chithras@ssn.edu.in*

Abstract
The Internet of Things (IoT) refers to system in which smart objects interact with each other with the aid of sensors and actuators through wired/wireless connection. When an IoT concept is implemented for real life application, the possibility of the system being attacked increases. The security measures have to be improved to prevent the attacks. This paper introduces light weight security schemes for authentication and encryption. This system uses Blom's scheme for authentication and Elliptic curve cryptography for encryption. Both these schemes are claimed to be light weight and hence is applicable of IoT applications which is a constrained environment. These security schemes are applied for healthcare system. The system is proved to be strong against the security attacks.

Keywords: *IoT, Blom, Ecc, Security and privacy.*

1. Introduction

Internet of things is emerged when embedded system is connected to the Internet. In this, everyday objects that are connected should be able to identify themselves with a unique Id, when connected to the internet. These everyday objects include fan, refrigerator, light bulbs which are connected to sensors and actuators. All these are connected to the internet. For example, in smart city, the sensors and image processing unit are connected to the vehicles and traffic signals which in turn are connected to the traffic control center.
When sensors are connected across the city in wide area, security concern occurs. Considering that IoT environment is dynamic in nature possibility of attacks are high. Sensor data can be intercepted or altered. Network security can be breached. Since, sensor data from militarized zone or health parameter are critical, data that are sent through the network must be encrypted so that critical data can be protected. We must also ensure that only authenticated person has access to the critical data.
Attacks on IoT devices are common to that of the wireless sensor networks. Some of the attacks in IoT are Botnets, man-in-the middle attack, data and identity theft, social engineering, denial of service attack. The security challenges can be overcome by using key management, encryption and authentication schemes. When selecting the encryption and authentication algorithm we must ensure that the algorithm is light weight.
Light weight protocols are used in memory constrained environment like system which use RFID tags, sensors, actuators. They are battery powered and the security algorithms which are used takes longer execution time (computational head), power consumption becomes higher. IoT networks are placed in potentially vulnerable locations and are highly prone to attacks. Some of the previously available algorithms which are used in wireless sensor networks are not usable in IoT environment. Though RSA, AES128 algorithms are being used, there are certain drawbacks with them. Drawbacks of RSA algorithm include,

- Users has to select a relatively small prime number
- Prime numbers chosen must not be of close values
- Two people cannot choose same prime number.

This paper illustrates the impact of using security schemes for protecting the IoT application. In this paper, Blom's algorithm is used for authentication and Elliptic Curve Cryptography (ECC) algorithm is used for encryption.

2. Literature Survey

This paper [1] says the difficulty faced when applying existing cryptographic techniques to IoT networks. The traditional cryptographic techniques used in wireless sensor networks cannot be incorporated because of high number of interconnected device which increases scalability.
This paper [2] focuses on increasing the reliability of IoT. Mainly focuses on securing, privacy and Trust. This is applied to smart city application. Also focuses on how the sensed data are protected and accurately transferred. Data is securely transmitted keeping in mind the privacy.
A smart health care system [3] system based on AES128 encryption was built. Access is protected only by password. For securing critical data using just password is not really secure. Implementation of authentication mechanism was needed.
In the aggregation method [4] both indirect and direct trust are maintained. In this method, to save energy data are being aggregated. Since all the data follow same path, each nod has to be trusted. There is no central authority of trust here. It uses modified dempster Shafer theory of combining evidence. It can be used when there is uncertainty.
In this paper [5] for encryption XOR manipulation is used. It is a light protocol suitable for IoT. But prediction of keys used is possible when one keeps listening to the key pattern. It must also be ensured that plain text and the keys are almost of same length.

3.Proposed System

The main aim of the sysytem is to provide security and trust to the IoT system. The security of the system is ensured by authenticating the user and by encrypting the data. Trust score for

each node is given by X-Bar chart method. This method uses the recorded value of the sensor as its parameter. The recorded value here is sensor data from the health care kit. This value should be accessible only to authenticated user. Authentication of the user is done by Blom scheme. In this method a set of pre-established matrix and prime number along with the vector matrix of individual user is used to generate a private key. This private key along with the vector matrix of the user with whom communication has to be established is used to generate shared key. When shared key of both the users are same authentication is done. Physician can now access the health care server where patient's vital parameters are stored. The dignosis or the prescription that the physician sends contain critical information. These information while sending to the patient or to the database can be intercepd or altered. To prevent it from altering or intercepting a proper encryption mechanism is needed. For this ECC algorithm is used.

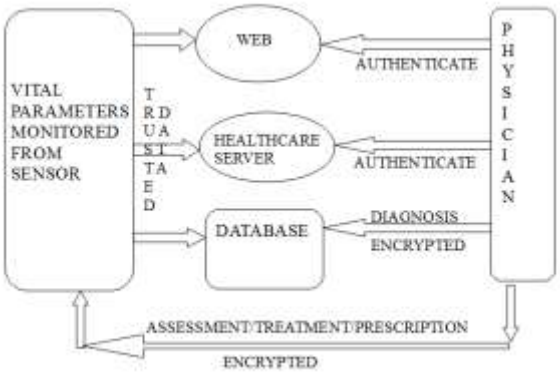

Figure 1: Architecture of Proposed Trust model

4. Encryption

Encryption was first invented as early as 1900 B. C by Greeks. In World War II, first break in encryption was detected. Encryption is securing data sent through the channel by any possible attacks. To secure data from being intercepted or altered secret keys are used to encrypt them. When the network or channel which are used to transfer data becomes vulnerable to attacks encryption algorithm is used.

4.1. Elliptic Curve Cryptography

ECC algorithm uses short key and requires less computational power compared to traditional encryption algorithm. This kind of algorithm is much suited for IoT environment. Since short keys are used memory limitation is eliminated. In ECC algorithm usage of lesser key size does not cmpromise on security. The equation of an ellipse is given by,

$$y^2 = x^3 + ax + b$$

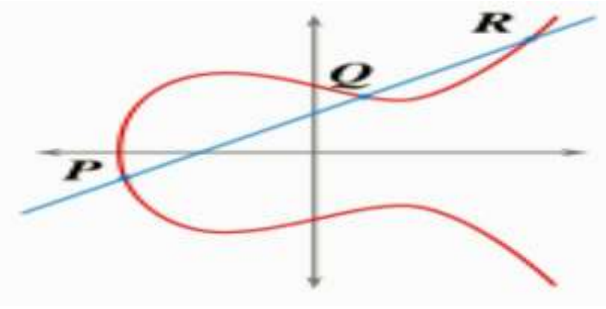

Figure 2: An elliptic curve

- Select a number 'd' within the range of 'n'.
- Generate public key with the following equation

$$Q = d * P$$

d= random number within 1 to n-1(Private key)
p= point on the curve
Q= Public key

4.2. Encryption

- The message m that is sent has to be represented on the curve as 'M'
- Select a number 'k' from [1 – (n-1)].
- Generate two cipher texts C_1 and C_2, Where,

$$C_1 = k * P$$
$$C_2 = M + k * Q$$

- C_1 *and* C_2 will be sent.

4.3. Decryption

Decoding the sent message in such a way that it is understandable is decrypting. A set of private or public key is usually used to decrypt the message. Here, using the formula given below decryption of the original message is done.

$$M = C_2 - d * C_1$$

Here C_1 and C_2 are cipher texts.M is the message sent and d is the random number that is chosen within n.Through the above equation decryption of the message is done.

4.4. Authentication

Usually, authentication involves using credentials to validate the users. This is done in human to machine communication. IoT involves machine to machine communication, which we need to ensure that the machine is authenticated to access data. Authentication involving credentials used in machine to human interaction is easy but vulnerable to attacks. Authentication which is more secure has to be used in machine to machine communication.
There, are two criteria which are considered when selecting the authentication algorithm. Firstly, the algorithm chosen must be lightweight and they must have less computational head.

4.5. BLOM'S Scheme

- Let p be a prime number greater than n. It is shared amongst the users.
- Let d = a square matrix of k*k elements mod p ,Where k is any value less than 5
- When adding a new participant, each participant chooses a vector matrix of k*1 dimension and its kept private.
- Private key is computed with vector and the symmetric matrix
- Now that private key of each participant is computed, shared key is generated by taking mod p.
- When both the participants have the same shared key, access can be given

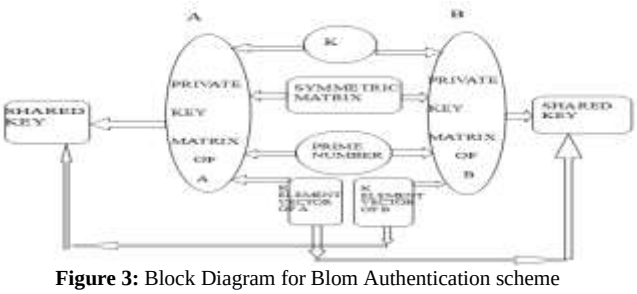

Figure 3: Block Diagram for Blom Authentication scheme

4.6. Trust Evaluation

Every process or a set of value has variations. In IoT a large number of data are being transferred .There may be deviations in the sensor data also. In order to make the system trust worthy, sensor data has to be analyzed. Control charts are used here for analyzing data.

With control charts, the data taken over a period of time are taken into consideration. There are basically two methods of control charts.

i. Control charts for variables
ii. Control charts for attributes

With control charts for variables a quality of data's attribute can be analyzed. Whereas, the later method helps in identifying the defects or number of defects.

$$\bar{X} = \frac{x_1 + x_2 + x_3 + x_4 + x_5}{5}$$

$$\bar{R} = maximum\ value - minimum\ value$$

Calculate the average of the averages

$$\bar{\bar{X}} = \frac{\sum \bar{X}}{N}$$

Calculate the average of range

$$\bar{R} = \frac{\sum R}{N}$$

Calculate Upper control limit (UCL) and Lower control limit (LCL)

Upper control limit= $ucl = \bar{\bar{X}} + A_2\bar{R}$

Lower control limit= $lcl = \bar{\bar{X}} - A_2\bar{R}$

Algorithm

dt – power utilized for transmission, dr – power utilized for reception, di – power utilization for idle time

```
Let x[n] be the values of sensor
For i=1 to n
begin
if(  min_value > x[i] < max_value )
Begin
For j=2 to n
begin
If(x[i] = x[j])
k++;
end
if (k = i-1)
energy= dt+dr+di
Trust calculation based on energy
else
Calculate Upper limit
Calculate Lower limit
Trust calculation based on X-bar chart
End
```

Every sensor node has an operational range. Firstly, this algorithm checks if the received value is within that range. Then, two possibilities may occur. The values received may differ or every value may be same. In case, all the values are same, battery power of the sensor is checked. If battery power is zero yet values are being received, appropriate trust score is given. If sensor values are different then X-Bar chart method of control chart is used.

In the x-Bar chart method, with set of values that is received an upper and lower control limit is set. Since this method is applied to a given set of values, trust score is very precise.

5. Implementation

Implementation involves collecting trusted data from health monitoring sensor. These data are stored and analyzed by server and the physician who is accessing the vital parameters through web must be authenticated.

MySignals HW (eHealth Medical Development Shield for Arduino) is a development platform for medical devices and eHealth applications. It has more than 15 sensors which can be used to monitor biometric signals. The sensor values that are used in X-Bar chart are recorded from the MySignals HW kit.

All the data gathered by MySignals is encrypted and sent to the user's private account at Libelium Cloud through Wi-Fi or Bluetooth. The data can be visualized in a tablet or smart phone with Android or iPhone Apps.

Through the health care kit, temperature values are sensed, 25 such values are recorded. These values are stored as a separate text file. The recorded values are used as input for calculating trust of the node. When recording the sensor values, initially it is checked if the values fall within the range of the sensor. Then, two cases are possible

CASE 1: If all the sensor values are same

Check energy of sensor. Sensors are all battery powered. As their energy decreases, the value which it sends may fluctuate or when sensor battery is drained it cannot send. This algorithm checks the battery power of the sensor if sensor keeps sending same values. If energy of sensor is good but keeps sending values, trust value is given accordingly.

CASE 2: If the sensor values vary

Now that the sensor values are different, these values are grouped into five subgroups containing five values each. These values are considered as input for X-Bar chart. From this trust score is calculated. This is done by reducing the trust score if values fall below or above the upper control limit or lower control limit of the X-Bar chart. These trust scores can be aggregated and whole trust score is given.

Table 1: Sensor readings

sensor	Sensor data					Average	Range
S1	36	37	23	38	42	35.3	19
S2	35	39.5	40	43	39	37.9	5
S3	42	41	28	39	16	39.8	9
S4	38	36	43	41	37	38.8	6
S5	37	9	38	39	36	37.2	12
						37.8	10.2

From the values of the sensor grouped in Table 1, average value of subgroup is calculated. The range of the sensor is the difference between the maximum and minimum value of the subgroup. These values are used to calculate the upper control limit and lower control limit. The upper control limit (UCL) is the highest range that the values can reach. The lower control limit (LCL) is the minimum value below which trust score of the system gets affected.

Control limit or centre line = $\bar{\bar{X}}$ = 37.8

Upper control limit = UCL = $\bar{\bar{X}} + A_2\bar{R}$ = 37.8+ (.58)10.2 = 43.716

Lower control limit = LCL = $\bar{\bar{X}} - A_2\bar{R}$ = 37.8-(.58)10.2 = 36.884

5.1 Accuracy

Accuracy refers to the degree to which the result of a measurement, calculation, or specification conforms to the correct

value or a standard. The table depicts how accurately the system works. Accuracy is calculated by categorizing the values into true positive, false positive, false negative and true negative. A value is said to be true positive if it comes under the range and estimated correctly. False positive is when the value falls out of range but the system says it is within range. False negative is if the value is within in range but the system predicts it to be wrong. True negative when the system projects the wrong values as mistake.
The total values that are considered for accuracy calculation is 25. These values are divided into 5 subgroups. The first subgroup contains three true positive values, a false negative value and true negative value. In the second sub group all the values are true positive. In the next sub group three values are true positive and two values are true negative. The fourth subgroup contains three true positive values, a false positive and negative value. The last subgroup has three true positive values, one false negative value and one true negative value.

$$\text{Accuracy} = \frac{\sum True\ positive + \sum True\ negative}{Total\ population} = \frac{17+4}{25} = 0.84 = 84\%$$

6. Conclusion

In this work, security and trust of a IoT is ensured. The system has been implemented with lightweight authentication and security schemes. Also, as a next level of providing more security for the system, the trustworthiness of the secured date is ensured using X-Bar chart mechanism. The significant advantage of this system is to provide a solution for the trade-off between security algorithms and memory constraint. The IoT systems are memory constraint system in which the implementation of light weight scheme has been implemented. This system has been tested with health care system as the application.

References

[1] Sicari, Sabrina, et al. "Security, privacy and trust in Internet of Things: The road ahead." Computer Networks 76: 146-164. (2015)

[2] Lee, Jun-Ya, Wei-Cheng Lin, and Yu-Hung Huang. "A lightweight authentication protocol for internet of things." Next-Generation Electronics (ISNE),International Symposium on. IEEE, (2014).

[3] Pöhls, Henrich C., et al. "RERUM: Building a reliable IoT upon privacy-and security-enabled smart objects." Wireless Communications and Networking Conference Workshops (WCNCW), 2014 IEEE,(2014).

[4] Bhoomika, B. K., and K. N. Muralidhara. "Secured smart healthcare monitoring system based on IoT." International Journal on Recent and Innovation Trends in Communication 3.7: 4958-61 (2015).

[5] Du, Wenliang, et al. "A pairwise key predistribution scheme for wireless sensor networks." ACM Transactions on Information and System Security (TISSEC) 8.2: 228-258 (2005).

[6] Chithra Selvaraj, Sheila, "Peer Profile Based Trust Model for P2P Systems using Genetic Algorithm", Peer-to-Peer Networking and Applications 5:92–103, DOI 10.1007/s12083-011-0111-9, volume 5, p92-103 (2012).

[7] Bhalaji N., Selvaraj C. "Comprehensive Trust Based Scheme to Combat Malicious Nodes in MANET Based Cyber Physical Systems, Advances in Intelligent Systems and Computing", *vol 508*. Springer(2017).

[8] Chithra Selvaraj, Sheila, "A Role Based Trust Model for Peer to Peer Systems Using Credential Trees", International Journal of Computer Theory and Engineering, Vol.3, No.2, , ISSN: 1793-8201(2011).

[9] N.Bhalaji, Dr.A.Shanmugam "A Trust Based Model to Mitigate Blackhole Attacks in DSR Based MANET" in European Journal of Scientific Research, Vol.50.No.1. 2011. Pp 6-. ISSN 1450-216X/1450-202X (SJR=0.034) (2014)

[10] N.Bhalaji, Dr.A.Shanmugam " Dynamic Trust Based Method to Mitigate Greyhole Attack in Mobile Adhoc Networks" (ICCTSD'11) Procedia Engineering pp. 907- 914,(2011).

[11] Li H, Singhal M (2007) "Trust management in distributed systems", 0018-9162/07 IEEE Journal – Feb (2007).

[12] Song S, Hwang K, Zhou R. "Trusted P2P transactions with fuzzy reputation aggregation" Published by the IEEE Computer Society 1089-7801/05, (2005).

[13] Aman Kumar, Dr. Sudesh Jakhar, Mr. Sunil Makkar "Comparative Analysis between DES and RSA Algorithm's" International Journal of Advanced Research in Computer Science and Software Engineering, JULY (2012).