Implementation of Security Layer on IoT based Sensor Network for Mission Critical Application

[1]Mr. Ratul Chowdhury, [2]Prof. Samir Kumar Bandyopadhyay
[1] Assistant Professor, [2] Professor
[1] Department of Computer Science and Engineering
[1]Future Institute of Engineering and management, Kolkata, India

Abstract: Internet of Things is a paramount research domain now. This technology ensures the end to end data delivery for any class of heterogeneous devices. For IoT application several methodologies had been addressed to secure the data available from sensor nodes, but most of them are based on social network paradigm. The mission critical application for tactical environment and the level of security measure have not been emphasized in most of the situation. This work primarily focuses on the state of art design of a security layer for mission critical application. A noble light weight security algorithm has been proposed and evaluations are made on real time test. Further the performance of the algorithm for real time data encryption has been discussed.

Index Terms **- Internet of Thing; Encryption; Perception layer; Sensor node**

I. INTRODUCTION

Due to the advancement of the Internet Technology the feature of the network architecture has been extended to an integrated multi object infrastructure. The data that are produced by several devices can be deployed and broadcast directly. Since IoT philosophy supports heterogeneous class of device, "things" and the services are in a common umbrella so the data may come from anywhere and can be redirected to any direction. Under these phenomena an obvious question may arise that whether the applicability of Internet of Thing is justified for any mission critical and tactical application? As the data come from heterogeneous things the security of the entire network and the service may be compromised to some extent. It is said that "Internet of Things is something like a home with millions of window and doors". If attackers smash a single window they get access to the network which leads to wide spread chaos. Data elements like border surveillance data, Statistics of Army operation in some terrorist infested region, and health statistics of Army personals during the mission are the classified information. Transmission of such information is really a critical issue. Several security measures have been implemented and addressed by considering such tactical scenario. Investigation the security level of classified data, more formally the classified health information of group leader and other soldiers and finally proposed an optimum method of security of the data from battle field to base station is the main subject of interest here. In this work our primary focus is to implement a security sub layer in perception layer of the IoT framework where physical sensors have been deployed. Here the on board encryption on data has been made in a hostile environment. The encryption has been done over the real time data stream hare to ensure a strong security over the mission critical information.

II. LITERATURE REVIEW

Several researches have been made in advancement of the real time health monitoring application. BSN Care [1] proposed by gopeet. al. Is an application of IoT in smart health care where bio sensors are implanted on patient body and if any abnormalities in body parameter found, the concerned people have to be reported immediately? Hassanalieragh et.al.[2] describes opportunities and potential challenges of health monitoring and management in IoT based scenario including cloud based processing a three layers architecture has been reported namely data acquisition, data transmission and cloud processing. A potential challenge on energy efficient sensing and energy efficient communication protocol design challenges has been addressed. Jara et.al. [3] have proposed an interconnection framework for IoT based m-health and remote monitoring strategy. CodeBlue [4] is another project done in Harvard Sensor Lab. It is primarily a medical telemetry system based on IEEE802.11 Architecture. It is highly applicable for remote monitoring of patient as well as in disaster hit regions. In such case an Ad Hoc implementation of the system is possible. Battle field medical information system network [5] is an approach of deployment of Bio-sensor in a tactical environment. That provides a direction towards tactical health care information management.

Since data security in tactical scenario has not been addressed in most of the work, therefore to bridge the gap between the data transmission and the data security in perception layer a new state of art security protocol has been proposed which ensures a strict security on the mission critical sensor data.

III. IMPLEMENTATION OF SUB-LAYER

To visualize the operation of the system the fundamental layered approach of IoT environment [6] has been considered, where the base layer acts as perception layer that grab data from the world and send them to network layer. From network layer the data has been broadcast to the application layer where end user and data analysis tool will handle the data elements. In this model perception layer is actually divided into two sub layers as shown in Figure 1. The bottom layer is the physical medium which is responsible for getting analog information of the world. Here typically multi sensor system has been deployed as a wearable device. Data captured by the device stored in a persistent buffer and sent to the encryption sub layer. The sub layer directly fetches the data form buffer and sent to the security sub layer. Security consists of a protocol that directly performs encryption to the sensor data. The encryption algorithm has been divided into 3 levels. Block level manipulation, intermediate steps and bit level manipulation.

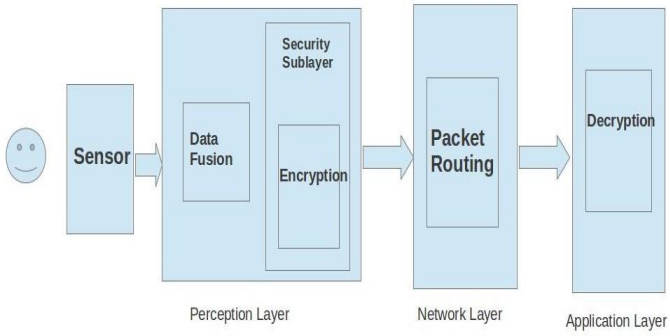


Fig. 1. Layered Architecture

In block level manipulation, the real time data stream is divided into 32bit block sequence and according to the value of a secret key k, the initial block sequence has been transformed into kth permuted sequence. The secret key has been prepared from a random number generator and it size varies between minimum 10 to maximum n! Number of digits.

To perform this block level manipulation, a permutation function has been used which transforms the initial sequence into kth sequence with respect to its positional value.

In intermediate steps, bit shifting and XOR operation has been performed in each block level. The bit shifting has been performed by considering the bit value of the key. Let us assume the key value produces is '54132' and consecutive 5 characters of a 32bit block sequence are 'D, B, A, C, H' sequentially. According to the methodology, D, B, A, C, H will be shifted right 5,4,1,3 and 2 times respectively and the new character sequences will become I, F, B, F, J. After completing one round, the same key value has been used in a circular basis for the rest of the character within a block. Each character within a block is further divided into 32 sub blocks, to perform the XOR operation. Each sub-block basically consists of the corresponding 8 bits binary equivalent of that particular character. Based on the secret key value one sub block remains unchanged. The XOR operation has been applied in each sub block with that unchanged block and reconverts the binary equivalent into initial character sequence after the end of the operation.

Finally, the bit level manipulation has been done based on the value of the secret key, each 32bit block sequence has been transformed into a random sequence by using the same permutation function. The entire operation has been mentioned in Figure 2.

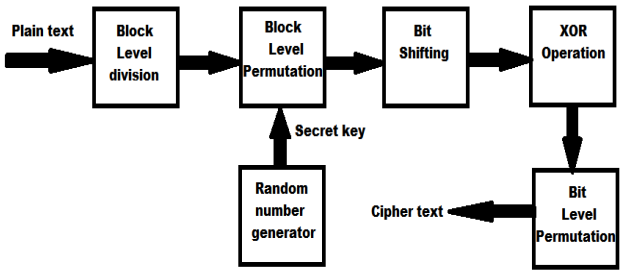


Fig. 2. Encryption Methodology

In application layer a simple decryption algorithm will reconvert the data into its original form, which is further use for analysis purpose.

IV. PROPOSED METHOD

The perception sensor nodes are the elementary component of perception layer. We have used open source microcontroller to implement it [7]. The sensor node can be deployed with a concept of device to cloud [8] methodology. The figure 3 depicted the single unit of the node. The node having four major components

- Temperature Sensor: Body temperature has been taken by using LM35 temperature sensor. It is a precision integrate circuit based temperature sensor. The centigrade temperature value given by the sensor is proportional to the output voltage. No additional calibration required for temperature measurement. However, for more precise operation and to make the temperature sensor work as a body temperature measurement device we are using a sophisticated calibration methodology. Although TO-92 plastic package of LM35 is having slower response time but is work more precisely in the temperature range -40degree C to +150degree C. we can use a metal coating over the TO-92 package to get much faster response. We have made a taping provision to mount them in various part of the body.
- Arduino Microcontroller: It is an open source microcontroller board driven by ATMega328P, a 8 bit microcontroller unit. It having 14 digital PWM I/O and five Analog Input pins. It runs with a clock speed of 16MHz. A more sophisticated version of Arduino can also be used known as Arduino Mega2560. Sensors can be interfaced within digital or analog pins. There is numerous hardware component can be added to extend the functionality of Arduino. These plug-in components are called shield
- Data logger: This is an additional part of the device that can store the temperature data in storage. The encryption has been done on this data as it stores on the device. After certain interval of time the data has been fetched by the encryption module

and it generates an encrypted packet of data which is considered as stream of characters. These data have to send to the base station by using a single channel 433MHz radio transmitter unit.

- Radio transceiver system is a single channel 433MHz RF transmitter receiver unit. The maximum range of the unit is 500 meter by introducing additional power to the receiving side. The transmitter unit send the in form of packet stream which is nothing but similar to character sets. In Arduino platform the virtual wire library has been used to transmit and receive encrypted data stream.

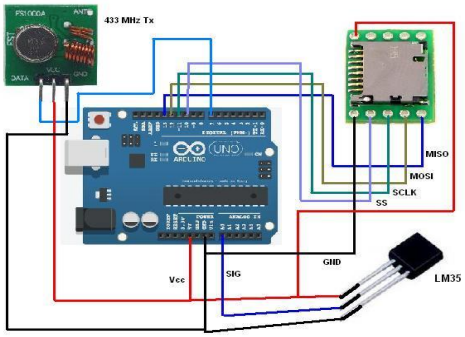


Fig. 3. Perception Layer Node

At room temperature of 0degree Celsius(C) the surface of the body temperature varies within 28 to 31degree C whereas at room temperature 28degree C it varies 31 to 34 degrees C. we have placed the temperature sensors in the location such as wrist, axillary and throat. The figure above depicted the body map and the sensor deployment point. The device itself is a wearable device and the data that has been sent by the sensor is analog. Body temperature that has been taken for from various point of human body is fused in the microcontroller through analog input pins. Central limit theorem methodology [9] has been used to perform fusion on the temperature data. The theorem says if x1 and x2 … xn are the n sensor measurement with noise variance σ21 and σ22 respectively and the combination of the measurement can be obtained by xn= σ2n(σ -21 .x1+ σ -22 .x2+ … +σ -22 .xn) where σ2n = (σ -21+ σ -22+ … + σ -2n)-1 is the variance of combined estimate. Final result of fused value is simply linear combination of n measurements weighted by their respective variances.

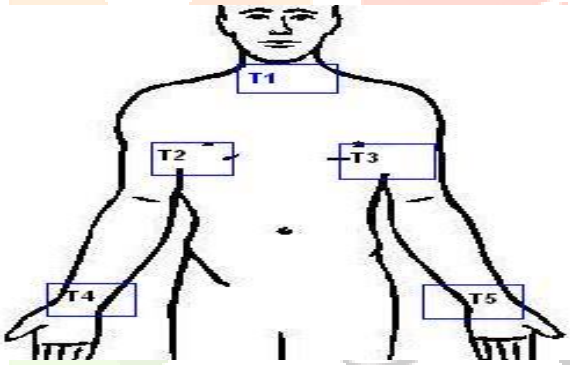
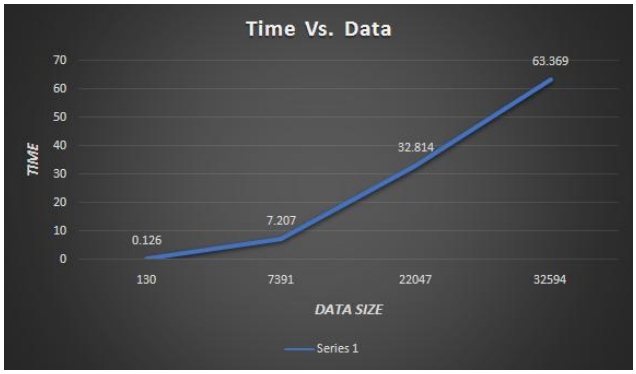


Fig. 4. Sensor Deployment Zone

V. Result Analysis

Performance analysis of the Encryption algorithm in security layer is the primary objective here. The key advantage of the proposed algorithm is that it is a lossless encryption technique and the level of security will increase gradually with the increase in the size of the data set. Each steps of the algorithm provides a level of security. In block level permutation if n number of blocks has been prepared from the dataset then to track the actual sequence requires to check n! different possible combinations. In second level since each key value can range between 0-9, therefore each bit within a block has a possibility so shift 0-9 times. In third level, an XOR operation has been applied on 32 sub blocks keeping one block unchanged, so each sub block has a possibility to perform XOR operation with the rest of the 31 sub blocks. Finally, the bit level permutation has been performed in each block. Based on the key value, a random sequence has been prepared from 32! different possible combinations. Without knowing the secret key 32! Combinations need to check to reach to the actual sequence. Combination of all four level increases the security of the proposed method in a higher semantic level. The graph depicted in Figure 5 and 6 describes the execution time for proposed encryption strategy and the conventional RSA methodology. The graph depicted in Figure 5 (a) and (b) describes the execution time for proposed encryption strategy and the conventional RSA methodology respectively. In case of proposed method for data size 22047 units the execution time taken is 32.814 Sec, if we apply RSA algorithm on the same data (22047 units) it will take an average time of 486.523 second. As the size of data increases to 32594 units the difference between the execution time is even higher. In this case proposed method takes 63.369 Second where RSA takes 677.572 Second. From the graph it is clear that our proposed methodology out performs the conventional RSA strategy. It is observable that as the data size (no of character) increases the execution time is increasing in exponential order conventional techniques like RSA. Whereas the execution time is increasing not too much rapidly for the proposed algorithm, which is definitely ensures a better performance in context of data security. The claim is even stronger in the light weight platform like senor node which has been deployed in a hostile environment where the time is a critical factor.



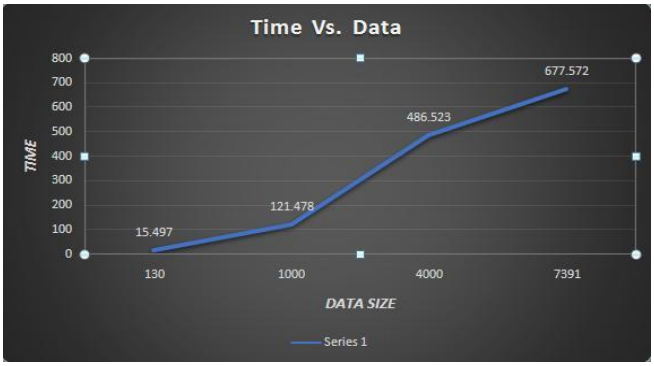


Fig 5(a) and (b) showing the average time taken to encrypt the data

The real time data before encryption and after encryption has been shown in figure 6.

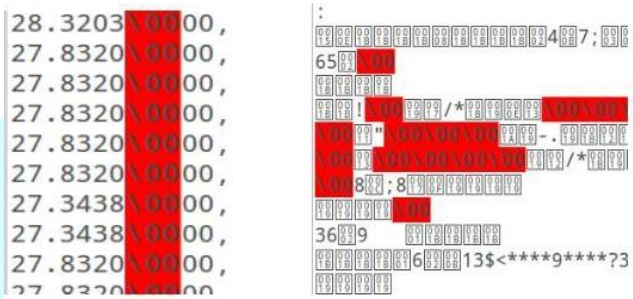


Fig. 6. Real time dataset before (left) and after (right) encryption

VI. Conclusions

We have shown a state of art security methodology for IoT based device in a mission critical scenario. The concept has been tested in a real time test environment and observed its efficiency with respect to classical cryptography technique. We can further apply the same methodology in more than one layer of IoT abstraction to confirm even higher degree of efficiency in the context of security. We will work further on multilayer security approach for IoT based on the same concept that ensures more secure data transmission framework for IoT based mission critical application.

VII. Conflict of Interest

We declare that there is no conflict of interest regarding the publication of this paper.

VIII. Data Availability

The data used in this paper are based on survey conducted over in a high way at the toll point in India. Some other data set are collected in the city of Kolkata, India. It is taken over a month.

References

[1] Gope, Prosanta, and Tzonelih Hwang. "BSN-Care: a secure IoT-based modern healthcare system using body sensor network." IEEE Sensors Journal 16.5 (2016): 1368-1376.

[2] Hassanalieragh, Moeen, et al. "Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges." Services Computing (SCC), 2015 IEEE International Conference on. IEEE, 2015.

[3] Jara, Antonio J., et al. "Semantic web of things: an analysis of the application semantics for the iot moving towards the iot convergence." International Journal of Web and Grid Services 10.2-3 (2014): 244-272.

[4] Malan, David, et al. "Codeblue: An ad hoc sensor network infrastructure for emergency medical care." International workshop on wearable and implantable body sensor networks. Vol. 5. 2004.

[5] Morris, Tommy J., et al. "Battlefield medical information system–tactical (BMIST): the application of mobile computing technologies to support health surveillance in the Department of Defense." Telemedicine Journal & e-Health 12.4 (2006): 409-416.

[6] Uckelmann, Dieter, Mark Harrison, and Florian Michahelles. "An architectural approach towards the future internet of things." Architecting the internet of things. Springer Berlin Heidelberg, 2011. 1-24.

[7] Tanner, Meghan, Ryan Eckel, and Indrajith Senevirathne. "Enhanced low current, voltage, and power dissipation measurements via Arduino Uno microcontroller with modified commercially available sensors." APS March Meeting Abstracts. 2016.

[8] Dey, Nilanjan, and Amartya Mukherjee. Embedded Systems and Robotics with Open Source Tools. CRC Press, 2016.

[9] Xing, G., Tan, R., Liu, B., Wang, J., Jia, X., & Yi, C. W. (2009, September). Data fusion improves the coverage of wireless sensor networks. In Proceedings of the 15th annual international conference on Mobile computing and networking (pp. 157-168).ACM.