International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT1952146

Data Security and Shortest Path Finding in IOT

W. Winfredruby[1], S Sivagurunathan[2]
[1]M. Phil Scholar, The Gandigram Rural Institute (Deemed to be University), Tamilnadu, India
[2]Assistant Professor, The Gandigram Rural Institute (Deemed to be University), Tamilnadu, India

ABSTRACT

Nowadays with the rapid growth of the smart city and the internet of things applications are difficult to connect the data access center, to meet service requirements with low latency and high quality while sending and receiving data access requests. At the same time, lower security performance occurred. In temperature and humidity sensor applications we approach a cryptography technique to protect data. It is an ASCII values-based technique which uses some numerical calculation to perform encryption and decryption. Then the use of the shortest path algorithm we find an entire possible path using current node detail and the destination node is sent by the source node to the neighbourhood nodes. Neighbourhood node receives the detail and checks the destination node. In case, the neighbourhood node is not the destination, it appends its detail along with the received details and sends to its neighbourhood nodes and the process continues till reaching the destination. By calculating the link delay between the two nodes. We can find the delay time taken from source to destination. At last we display the entire possible shortest paths and secure data. It is useful when network congestion occurs. In this paper, we also overcome this problem.

Keywords: Data access center for the Internet of things. ASCII Values. low latency. Shortest path algorithm. Network congestion.

I. INTRODUCTION

The development of the internet of things technology receives attention in many applications. Many countries consider the IOT as an important strategic component of emerging industries [1] and have adopted a number of policy measures to comprehensively promote the development of these applications in various fields and will deeply integrate and generate new types of IOT solutions.

The huge number of embedded devices that can interact with the environment are connected to the internet. The development of such an interacting object reaches this staggering pace with the growth of microcontroller based easy-to-use designed system, which is substituted for old system design with complicated electronic circuits.

The temperature and humidity monitoring sensors are common to measure environmental conditions. In our paper, we process a measured temperature and humidity by sensing and display on the computer screen. A merged temperature and humidity sensor DHT11 are used with Arduino Uno to develop Celsius scale thermometer and percentage scale humidity measurement process.

A major prohibition against distribution of these applications is the difficulty in product QoS over the internet. MPLS selection is to find the shortest path. This path is affordable whose end-to-end delay is bordered by the delay requirement of time-sensitive

data flow. Dijkstra's algorithm computing the shortest path can be used in many circumstances.

There are two schemes implementing the QoS routing algorithm on routers. The first one is to implement as an on-line algorithm to process the routing request as they appear. It is not always desired. The second one is extending a link-state protocol and the cheapest delay-constrained path for the destination. These approaches provide assist to both constrained unicast and multicast. In this paper, we approach the second one to find the feasible path that satisfies the delay requirement. There have been some solutions to this problem. However, there is no known algorithm to find a path in polynomial time.
There are several algorithms which have different ways to encrypt and decrypt the data using various type of keys. These algorithms are divided into two major categories from the basis of the keys. There are symmetric and asymmetric algorithms. The same key for encryption and decryption is called symmetric. Asymmetric decryption uses different keys for encryption and decryption. Asymmetric cryptographic algorithms are RSA, Digital signature, etc.., Semantic algorithms are stream cipher, RC2, RC4, RC5, DES, Block Cipher [2].

The major task of these algorithms is to perform encryption and decryption and then provide security from attacks. Every time attackers try to attack the information to get it to destroy it by various types of attacks. These attacks are divided into two categories passive and active attacks.

The passive attack is of two types. one is learning the contents of transmission, and the second one is traffic analysis. The active attacks are involved in some modifications of data. In these active attacks are classified into four categories: Masquerade, Replay, Modification of data and Denial of service [3].
The rest of the paper contains follows: Section 2 explains related work; Section 3 Explains Materials and Methodologies used, Result and discussion are explained in Section 4; In section 5 Conclusion and Future work are presented.

II. RELATED WORK

The main focus of current research on service access requests under the condition of sufficient static resources. static resources. Norberta et.al., have proposed a paper on the development of a wireless sensor monitoring system for humidity and temperature in the Civil structure [4]. Li et.al., have made a survey on how IoT has an impact on industries. They have mentioned that IoT has provided a promising opportunity to build Industrial systems in a powerful manner and a wide range of industrial IoT applications have been developed in recent years [5]. Jayavardhana et.al., have surveyed about the vision, architectural elements and future direction of the Internet of Things. In the IoT application, we concentrate on data access with security [6]. Ning et.al., have proposed an efficient authentication scheme and a scheme for access control for the Internet of Things. In our proposed work, we have implemented data integrity using ASCII value based on encryption and decryption for secure data access along with the shortest path algorithm for data transmission [7]. Suraj et.al., have proposed ASCII based encryption a decryption technique for information security and communication. They have mentioned that this is one of the hard methods of information security [8]. Akancha has proposed an ASCII value-based data encryption algorithm and it has compared this algorithm with other symmetric data encryption algorithms. In our proposed work, we are dealing with source data access in humidity and temperature sensing applications [9]. Ying Xiao et.al., have made a study about constrained shortcut path patterns. It will relatively reduce the transmission time of the packet [10]. Crauser et.al., have proposed a simple criterion which Dijkstra's shortcut path algorithm

into a number of phases, where all their processes are run in parallel. In our, proposed work, we have used Dijkstra's shortcut path algorithm to find the shortest path for the transmission of data [11]. Yi Mang et.al., have proposed an algorithm for distributed research aware data access algorithm based large scale access to security of data transmission. In our proposed work, we are concentrating on the security of data transmission/data access [12]. Ferrando et.al., have written an article on a constraint-based path selection algorithm [13]. Above mentioned studies have solved a respective application environment by matching access problems and create limitations. In our proposed work, we have implemented a secure data accessing scheme for humidity and temperature seeming system which is one of the very popular IOT applications. We have implemented security measures such as ASCII value-based encryption and decryption technique in order to ensure data integrity during transmission. We have also used Dijkstra's shortest path algorithm for data transmission.

III. MATERIALS AND METHODOLOGIES

3.1 Materials

3.1.1 Arduino

Arduino is the main part of this building monitoring system. It is also be defined as a single board microcontroller for building digital objects and interactive devices. It is designed to sense the environment by receiving input through sensors. This is available in many formats and designed enabling different features. This software can be run on Windows, Linux or Mac. This program is based on hardware wiring.

It can be programmed to stand-alone, with the computer. It is a microcontroller board, based on an 8-bit microprocessor. There are 15 input and output pins. It has a USB to connect to a computer or Raspberry Pi.

3.1.2 Sensors

Sensors are the electronic devices that convert a change in physical phenomenon into an electronic signal. It can send information to the computer. The sensor is used in robotics, airplanes and aerospace, cars and many applications. In our paper, we used temperature and humidity sensor-DHT 11. It is relevant in heating, ventilation and air conditioning. Fig 3.1.2 shows the combined Arduino Uno and DHT 11 sensor Boards.

DHT 11 has the following performance range and accuracy.

The range of Measurement:
Temperature-10 to 80^0 C
Humidity 10 to 90% RH
Accuracy Range:
Temperature±1%
Humidity±6%

The amount of water vapor contained in air is defined as humidity. The ratio of the water vapor content is denoted as Relative Humidity (RH).

$$RH=\frac{\rho w}{\rho s} *100\ \% \qquad (1)$$

ρw - Density of water vapor
ρs – Water vapor Saturation

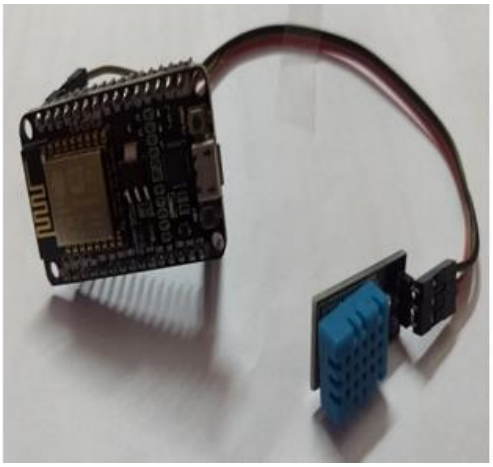

Fig:3.1.2 Combined Arduino Uno and DHT 11 Sensor Board

3.2. Methodologies

3.2.1 Dijkstra's Algorithm

It is an algorithm that is used to find the shortest path or minimum cost and is represented in the graph. In this algorithm first, start at the ending vertex by making it with a distance of 0. It is 0 units from the end. It is called the current vertex. All of the vertices are connected to the current vertex with an edge and calculate their distance. Note each distance with their corresponding distance. If it is less than the previous distance visits the vertex and note the new one. Continue these processes until the shortest path is found.

Delay Estimation

The focus of this work is to know, how end-to-end measurement can be used to network infer per-link delay. Particularly attention will be paid to the probability distribution estimation of the pre-link variable delay. The logical model for the physical network is to define strategic direction, which is called the tree model.

The estimation is not focused on the physical propagation delay, because it doesn't determine the behavior of the network in a critical way and a more manageable value than the additional variable delay attribute to other processing or queuing in the buffer in a router.

The deduction strategy is aimed at the approximation of the variable delay previously mentioned and extended from the estimation of end-to-end delays acquired by the end-to-end measurements to the events of the network, Such as per-link delays. Realizing these quantities, it is feasible to define the delay distribution for the individual link by using only the measured distributions of end-to-end delay of the multicast or unicast packets.

The next segment describes a logical model for studying a network topology, which is called a tree model. A physical network is restored by a logical tree composed of a root and the branch nodes that get down from the leaf receiver node.

The distribution delay of an internal node delay is very complex. It is acquired by analyzing the different ways. In the end-to-end delay can be split between the portion of the path below or above the node. The key expectation is the per-link delay between different links and packets independently. The packets are potentially subject to lose over and queuing each link.

3.2.2 ASCII-Based Encryption

When we need to send data to the network, it should be encrypted in order to ensure security during transmission. In our proposed work, we use ASCII - value based encryption. In our encryption technique, at first, the ASCII value of the input message is set to a variable c. Next encryption key is generated using the formula,

Encryption key_c = ord (key [i % len(key)]) (2)

Next, the encrypted data is generated using the formula,

Encrypted data = char ((msg + key) % 127)(3)

Finally, the ASCII letter of the encrypted value is displayed. Fig 3.2.2 shows the flow of ASCII-Based Encryption method.

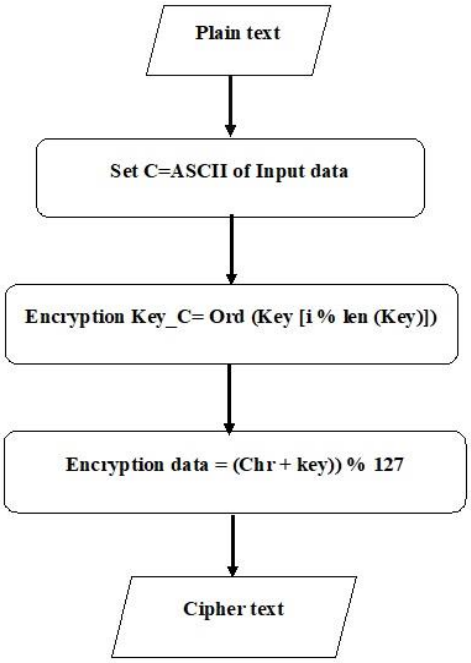

Fig 3.2.2 Flow chart of ASCII-Based Encryption

3.2.3 ASCII-Based Decryption

After encryption data is received by the destination, the following operation is performed to obtain the decryption key.

$$\text{Decryption key} = \text{ord}(\text{key}[i \% \text{len}(\text{key})]) \quad (4)$$

Next, the decrypted message is generated using the formula,

$$\text{Decryption data} = ((\text{Cipher text} - \text{key}) \% 127) \quad (5)$$

Finally, the ASCII letter of the decrypted message is displayed. Fig 3.3.3 shows the flow of ASCII-Based Decryption method.

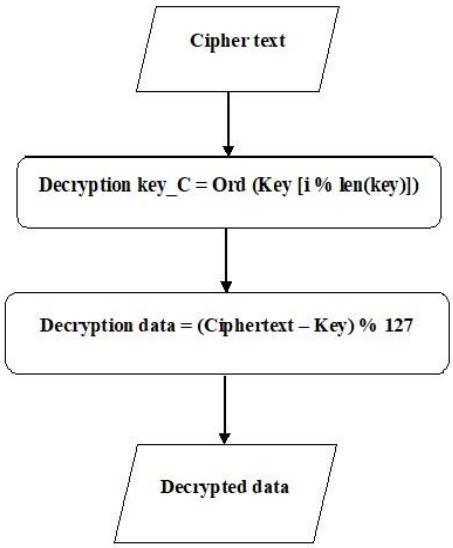

Fig 3.3.3 Flow chart of ASCII-Based Decryption

IV. RESULTS AND DISCUSSION

In our work, we used Dijkstra's Algorithm and ASCII based encryption and decryption combinedly. This experiment was done by Intel Core i5 CPU @ 1.90 GHz with Windows Operating System, humidity and temperature monitoring sensor and the Raspberry Pi. We run the code on real devices without modification of the code or algorithm or protocol. At first, we have combined Arduino Uno and DHT11 sensor to monitoring temperature and humidity reading. After the monitoring, the readings are listed out and converted the ciphertext using ASCII based Encryption and decryption method. The converted ciphertext was sent via routers by calculating the shortest path using Dijkstra's algorithm. The sent data after reaching the destination will be converted as plaintext (original data). Table 1 summarizes the process

Table 1 : Path finding process details

S. no	Name of the sensors used	Sensor Readings	Name of the algorithm used	Encryption Data	Shortest path nodes	Decryption Data
1	Arduino Uno, DHT 11	56,35	Dijkstra's shortest path Algorithm	4848484848	0→0 1→4 2→4 3→3 4→1 5→5 6→3 7→2 8→6	56,35

V. CONCLUSION

Previously, Yi Meng et al., have developed a data access algorithm for general IoT applications. They have mentioned that this algorithm did not optimize load consumption while transmitting data via a network. They have not implemented any security to the data during transmission. This may lead to data loss (or) loss of integrity of data. In our proposed work, we have used the shortest path algorithm to transmit the data along with security measures. We have used ASCII based encryption and decryption during data transmission which ensures data integrity. One limitation of our proposed work is that a time delay occurs when both the Shortest path algorithm and the Encryption and Decryption algorithm are executed simultaneously. In our future work, we will try to overcome this limitation.

VI. REFERENCES

[1] Da Xu, Li, Wu He, and Shancang Li. "Internet of things in industries: A survey." IEEE Transactions on industrial informatics 10.4 (2014): 2233-2243.

[2] Akanksha, Mathur. "An ASCII value-based data encryption algorithm and its comparison with other symmetric data encryption algorithms." International Journal on Computer Science and Engineering (IJCSE) 4.09 (2012): 1650.

[3] Stallings, W [2005]. "Cryptography and Network Security Principles and Practice," 4th Edition, Pearson Education-Prentice Hall, ISBN 10: 0-13-609704-9 ISBN 13: 978-0-13-609704-4.

[4] Barroca, Norberto, et al. "Wireless sensor networks for temperature and humidity monitoring within concrete structures." Construction and Building Materials 40 (2013): 1156-1166.

[5] Da Xu, Li, Wu He, and Shancang Li. "Internet of things in industries: A survey." IEEE Transactions on industrial informatics 10.4 (2014): 2233-2243.

[6] Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future generation computer systems 29.7 (2013): 1645-1660.

[7] Ye, Ning, et al. "An efficient authentication and access control scheme for perception layer of the internet of things." Applied Mathematics & Information Sciences 8.4 (2014): 1617.

[8] Suraj Arya [2017]." ASCII Based Encryption Decryption Technique for Information Security and Communication. "International Conference on Innovative Trends in Science, Engineering, and Management-(2017).

[9] Mathur, Akanksha. "A Research paper: An ASCII value-based data encryption algorithm and its comparison with other symmetric data encryption algorithms." International Journal on Computer.

[10] Xiao, Ying, et al. "The constrained shortest path problem: Algorithmic approaches and an algebraic study with generalization." AKCE International Journal of Graphs and Combinatorics 2.2 (2005): 63-86.
[11] Crauser, Andreas, et al. "A parallelization of Dijkstra's shortest path algorithm." International Symposium on Mathematical Foundations of Computer Science. Springer, Berlin, Heidelberg, 1998.
[12] Meng, Yi, and Chen Qinghai. "DCSACA: distributed constraint service-aware collaborative access algorithm based on large-scale access to the Internet of Things." The Journal of Supercomputing 74.12 (2018): 6408-6427.
[13] Kuipers, Fernando, et al. "An overview of constraint-based path selection algorithms for QoS routing." IEEE Communications Magazine 40.12 (2002): 50-55.

Cite this article as :

W. Winfredruby, S Sivagurunathan, "Data Security and Shortest Path Finding in IOT", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 2, pp. 551-557, March-April 2019. Available at doi : https://doi.org/10.32628/CSEIT1952146
Journal URL : http://ijsrcseit.com/CSEIT1952146