EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Analytical Method to Improve the Security of Internet of Things with Limited Resources

Abdul Hannan Khan[1,2,*], Shahan Yamin Siddiqui[1,2], Muhammad Sohail Irshad[2], Saif Ali[2], Muhammad Rehan Saleem[3], Shahid Iqbal[4]

[1]School of Computer Science, National College of Business Administration & Economics, Lahore, Pakistan.
[2]Department of Computer Science, Minhaj University, Lahore, Pakistan.
[3]Department of Computer Science, University of Management and Technology, Lahore, Punjab, Pakistan.
[4]Department of Computer Science & IT, Virtual University of Pakistan, Lahore, Punjab, Pakistan.

Abstract

This research is about the information security of very obliged gadgets. Design Science Research (DSR) Method is utilized for this reason. It let us pick up the fundamental thought and exploration of the primary issue space. This is a procedure of combining distinctive pre-affirmed examines to pick up the goal. Symmetric cryptography will be utilized as a noteworthy device in various information items and entryway gadgets. The principle target of this exploration is to give security to exceptionally constrained gadgets as they are not ready to convey utilizing TLS or DTLS given a deficiency of assets. This arrangement is a finished bundle to give credibility, information honesty and privacy, either information is making a trip to entryway, gadgets or the web. At the information interface layer, AES symmetric encryption is utilized and information questions likewise are encoded utilizing a similar encryption strategy. Assessment is performed using wire shark.

Keywords: Internet of Things (IoT), Design Science Research (DSR), Advanced Encryption Standard (AES), Transport Layer Security (TLS), Datagram Transport Layer Security (DTLS).

Received on 13 March 2019, accepted on 29 March 2019, published on 26 April 2019

doi: 10.4108/eai.13-7-2018.163502

1. Introduction

Internet of Things (IoT) refers to the devices that are growing day by day and helps improve the human facilitation level with their ability of connectivity and data processing in constrained environments also. These devices normally use web standards like HTTP, FTP, MQTT or CoAP that allows them to connect with the internet and share the data over devices and different networks like the internet or LAN. The protocols have increased the usefulness and accessibility standards of IoT devices. The data gathered by IoT devices is uploaded to cloud storage or servers for analysis and processing [1].

IoT devices are being popular now a day due to their abilities to access sensor-related data in different fields like medical, weather and security measures. The rapid development in mobile Wireless sensor networks and other fields like Radio Frequency Identification (RFID) and its integration with cloud storage and processing abilities had made its use more feasible for people. The IoT devices include a variety of cooperative mechanisms. These devices include a mobile phone, pc, tablet, PDA and other small handheld devices. These devices support cost-effective sensors that can receive and communicate data. This way these IoT devices are an important part of centralized systems that are growing rapidly with internet communications. The daily working routines are now part of the virtual world that is surrounded by these devices [2].

Micro devices like oven, refrigerators, ACs, fans, bulbs and home appliances are interconnected with the help of IoT devices. They communicate data with each other and can take decisions on the base of input. The cloud storage works on the backend of these devices where huge processing takes place for the sake of analysis. Home automation is based on these devices that allow building a system using intelligent architectures. The interconnection of devices is collectively called as IoT. The mobile control of these

*Corresponding author. Email:Hannankhan.cs@gmail.com

devices allows accessing them from distance using the internet [3].
Constrained IoT devices have low resources in terms of CPU efficiency, RAM and ROM and require battery efficiency. These devices have innate sensors that collect the data from the environment where they are deployed. Other use of these devices includes a machine to machine data transfer and small control mechanism used in home or industrial environments. These devices are often interconnected using a network therefore they are called things. This network is therefore called the internet of things. Such a network consists of embedded computers or smart devices that have sensing ability with data connectivity or data exchangeability. They can easily be connected to other devices of this kind of server [4].
A major issue that arises when data communication is done by IoT devices. The resource-scarce nature of these devices incorporates less secure methods that have few calculations involved in their operations. The functionality of such devices is restrained however resources are enough for basic operation of these devices but cannot be enough for calculation rich operations. The measure of available resources categorizes these devices. For such devices that are resource-constrained and do not has enough resources for calculation rich security operation is categorized as Class 0 IoT device [5].

2. Literature

Dave et. al. [6] described the idea of a system of keen gadgets was talked about as right on time as 1982, with an adjusted Coke candy machine at Carnegie Mellon University turning into the principal Internet-associated apparatus, ready to report its stock and whether recently stacked beverages were cold or not. In a resource-constrained IoT device security of data, communication is the main issue due to the limited security support of resources. Resources after performing the functionality in devices are still available. Class 0 devices are highly constrained devices and quantity and amount of available resources matters a lot in any IoT device of this class.
Hernandez et. al. [7] found that it is imagined that the Internet of Things (IoT) will upset how people and organizations collaborate with the advanced and physical world. Later on, IoT will be a piece of everybody's day by day lives by broadening the correspondence and systems administration abilities of physical items or keen gadgets. In this manner, IoT can be seen as an expansion of IT to all aspects of our lives; changing at present separated systems into new systems to frame a worldwide interconnected heterogeneous system of brilliant items or things.
Hu et. al. [8] described the Representational state transfer method. This protocol describes a standard web security measure for communication over the web. Other benefits of this method are its workability with different web protocols like HTTP and File Transfer Protocol. REST uses ATOM and JSON for data transfer over the web with high frequency. Sometimes XML is also used by REST services but not very frequently. REST operates on popular data transmission of HTTP. These methods include GET, POST, etc. IoT systems use REST for communications with the help of HTTP. CoAP is also used as an alternative by IoT devices.
Zhang et. al. [9] presented an analysis of HTTP security parameters. According to their statement, HTTP is no more a secure protocol as it sends data like a plain text without applying any encryption mechanism. To remove this con, there should be some encryption mechanism used by HTTP. Sending sensitive data in plain text format is not secure over the internet. Choices for securing the internet communication include SSL or TLS. TLS stands for transport layer security. A combination of these two algorithms is popularly known as HTTPS which allows cryptographic support. Other benefits of HTTPS include data confidentiality; data integrity checks and ensures reliable transmission.
Computational Intelligence approaches like Fuzzy system [10, 11, 12, 13, 20, 21, 22, 25, 27, 30], Neural Network [21, 24,25,29], Swarm Intelligence [22,25,31,32] & Evolutionary Computing [14, 15, 16, 23] like Genetic Algorithm [14, 15], Differential Evolutionary (DE), Island GA [17], Island DE [18, 19], Deep Extreme Learning Machine [25, 26, 28] are strong candidate solutions in the field of IoT enabled smart city [11, 12, 20, 24], IoT enabled Smart health [13, 25, 27, 30], Cryptography [33] and wireless communication [22,24,25,26,28] etc. Computational Approaches are hot research area which is also used in IoT based System.
Tan et. al. [34] mentioned these days, the fundamental correspondence structure on the web is human-human. In any case, it's obvious that in a very close-by shortly that something can have a motivating system for perceiving affirmation and may be cared-for with the target that every article will be connected. The web can progress toward obtaining the possibility to be to the web of Things. They provide structures that can produce from human-human to human-human, human-thing, and thing-thing (moreover referred to as M2M). This will bring another sure enrolling and correspondence amount and alter individuals' life incomprehensibly. Frequency Identification frameworks (RFID) and connected ID advances are the foundations of the conventional web of Things (IoT). This paper expects to demonstrate a skeleton of the web of Things and that we endeavour to handle some key problems with the web of Things like its structuring and also the ability, and then forth. Toward the beginning, we tend to portray a graph of the web of Things. By then we tend to provide our structure proposal of the internet. The Internet-of-Things and someday later we set up a specific web of Things application show which might apply to tweaked operating environments the overseers within the shrewd grounds. Finally, we tend to point out some open solicitation regarding the web of Things.

3. Proposed Methodology

The proposed security improvement of IoT model discussed in this section, the present work follows the needs of secure communication by IoT devices which have fewer resources

and hence they are not being able to implement heavyweight security mechanisms. The output of this research study will provide protected control for communication for the highly constrained IoT devices. For this purpose, we will deeply study the existing research works in this regard. The methodology chosen to complete this work is the Design science Research method. This method follows the actual problem to solve efficiently.

As the main purpose of this research is the security of IoT gadgets with constrained assets to oversee secure correspondence of information, numerous gadgets with rich assets are as yet enduring with real security issues. In an investigation of dangers to the protection of information and security from home machines, scientists inspected three mainstream gadgets. Explicitly the savvy broiler, keen security entryway and primary power switch of power. The consequence of the investigation finished by showing a powerless encryption, absence of proper validation, minds information uprightness and ramifications of security of these gadgets. Bormann et. al. [4] proposed a plan of characterization among obliged IoT gadgets for the sake of their accessible framework resources.

Table 1. Characterization of Constrained IoT Gadgets for the Benefit of their Framework Assets

Sr. No	Name of Class	Read-Only Memory Capacity	Random Access Memory Capacity	KB=1024 bytes
I	Class-0	<<100 KB	<<10 KB	
II	Class-1	~100 KB	~10 KB	
III	Class-2	~250 KB	~ 50 KB	

Table 1 clears up the projected request of IoT devices dependent on their open resources. Class-0 (C0) is a lot of resources forced so that they have the least various talents to assist secure correspondence over the framework. Class-1 (C1) has scintilla a bigger range of advantages than C0. The devices have a spot with C1 square measure to some extent ready to run shows of duty-bound correspondence, as an example, CoAP and DTLS or different transport layer security shows. As I documented they're to some extent ready to deal with these shows, therefore we are going to watch towards Class-2 (C2) for finishing TLS, FTP, hypertext transfer protocol or different net shows. This info is efficacious to select that security show must continue running over your to some extent, passing or conventionally duty-bound IoT contraptions.

RAM and ROM of class zero devices are very limited. RAM of these devices must be less than 1 MB and ROM should be less than 10 Mb. Arduino UNO is a microcontroller of 8 bit, it has 3.2 Mb RAM, 16 MHz CPU, and 0.2 Mb ROM. The size of the application code is equal to the size of ROM and RAM is used to process the operating applications of the device. In the presence of sufficient RAM, ROM is unable to perform the security mechanisms due to limited code space.

3.1 Design methodology

Design Science Research (DSR) method is followed in this article as it ensures a comprehensive understanding of the problem and help in discovering the solution. DSR is applied as a proactive model for problem-solving in this work. Solution results in a security paradigm for class 0 IoT devices and internet gateway. The system model is confirmed when the gateway is put to an experimental study involving class 0 devices. Results are observed for gateway and are used a proof of our proposed model. The system model is confirmed in this way. The process of design is divided into many steps that are discussed in the following. The basic step follows the design science, research model. The design methodology can be explained by using many models.

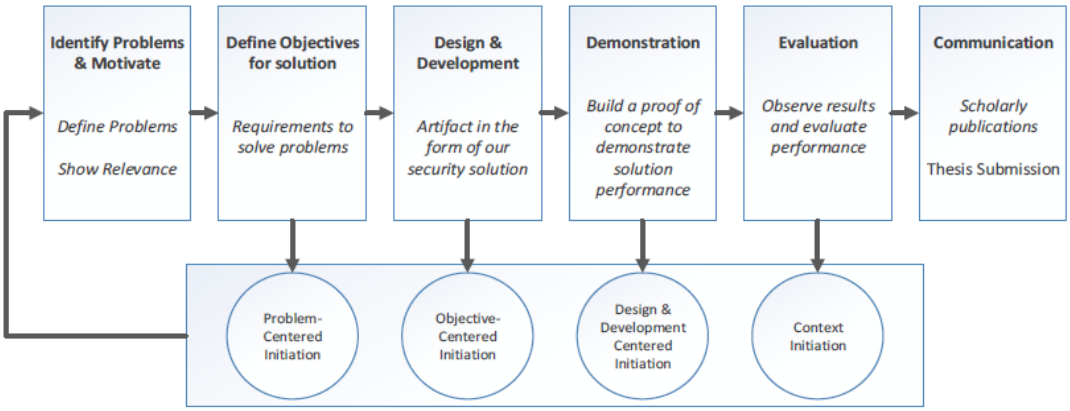

Figure 1. Design Science Research Methodology by Peffers et. al. [35]

3.2 Motivation and Problem Identification

This step is the first step in the method followed during this research i.e. Design Science Research Process (DSRP). The issue is identified in this phase. During this phase, the problem statement is identified and the following issues are noticed. Data communication security is focused as the major problem that is to be solved for highly constrained IoT devices. Other concerns are also considered as associated problems like data security at rest; however, the solution scope not follows them and is only centred on data security when the communication channel is active.

Table 2. Description of Problems

Problem Identification	Details of the Issue
1	Highly constrained devices cannot communicate in a secure manner
1.1	Highly constrained devices may communicate to the web but in an insecure manner
2	Security gateway can secure the communication partially, however security gap is left with the solutions
2.1	Gateways leave information that can be used for attack purpose
2.2	Communications between gateway and devices are not secure

Problem 1: Highly constrained devices cannot communicate in a secure manner

The devices cannot support the transport layer security (TLS) protocols when they are highly constrained. This suffers from the data communication channels. DTLS standard is a heavier standard as compared to TLS that why it needs more resources to be executed on highly constrained IoT devices. On the other hand, resources are not available in such conditions in highly constrained devices. This results in an inability to execute the DTLS standards.

Class 1 & 2 devices can have enough resources that can allow them to execute the DTLS standards. They can also have more memory to execute the TLS standard. 0.1 MB ROM and 0.001MB Ram is needed necessarily to execute these protocols. On the other hand, class 1 devices are constrained at these limits. Class 0 devices have low memory than class 1 devices and therefore we call them highly constrained. This Lack of resources results in the inability of supporting the security of data communication channels [36].

Problem 1.1: Highly constrained devices may communicate to the web but in an insecure manner

The IoT devices when they don't have resources that are necessarily needed for secure data communication, are unable to secure the data on the internet or over a network. However, they continue to communicate with other devices on the network without applying the security measures. This results in insecure communication over the network channel. This doesn't affect the success of the communication but the security of the communication. The insecure data is open for attack and creates the vulnerability of the communication channel. This vulnerability is not ignorable. This is considered a TLS level security problem. On the other hand, the issue is regarded in the 4th position among the top 10 security considerations of the IoT devices. These lists of the top ten security issues are generated by OWASP. According to OWASP, the information sending over the network should always be encrypted to avoid the attacks and it forbids the insecure channels over the devices. They follow through the security measurements that are made using SSL/TLS protocols. OWASP provides alternate solutions to the issues also. However, if insecure communication continues and the issues are not taken down, there is a risk of losing important data during the communication. Many other security solutions are proposed for avoiding data loss. There is a chance of losing the account information as well as the data stored or used by the account if the communication channel is not secure. Other security solutions mentioned are also helpful in securing the communication by class 1 and class 2 IoT devices but there is a problem for class 0 devices as they cannot follow these solutions due to their overhead. This leads to the necessity of finding an alternate solution that must be followed by the class 0 devices.

Objective 1. Security of data communication when transferred to destination form highly constrained devices

Confidentiality of data is necessary between the source and destination of webserver and highly constrained IoT devices. This way the data is secured between the two. The gateway can be put between the server and IoT devices. The transmission process is divided into two parts by this method. The transmission is done from IoT devices to gateway and then from the gateway to the destination Node. The transmission is governed by security protocols at every section differently. We can say that one part is governed by LAN protocols while the other is governed by WAN protocols. Therefore, it is necessary to use the correct transmission protocols for governing communication.

Objective 2. Security of data communication between the gateway and destinations

Data Communication needs to be protected strongly before the data is sent over the internet. A security layer needs to be established for this purpose. Security Gateway will be used to provide a wall to secure communication and avoid outside attackers. OWASP () recommend that DTLS or TLS protocol may be used to secure the data when it is transmitted over a network. This security may be governed using encryption techniques as mentioned by the OWASP. This will secure the communication channel from outside attackers and inside threats as well.

Objective 3. Security of data between the gateway and class 0 IoT devices

The data security is needed when the data travels from the IoT device to the security gateway. This part of

communication is dependent on class 0 IoT Device for its security of communication. As much power the device, the more secure the communication. A stronger protection can be made by applying the DTLS. IoT devices can make data encrypted that will result in difficulty to read. However, it's not possible to apply the DTLS protocol over the class 0 device. As the class 0 devices have fewer resources to maintain its calculation overhead. Therefore, an alternative solution is needed to fulfil the research gap that is necessary to provide data protection during communication and on the go.

3.3 Design

The third phase of the methodology is the design phase. This step finalizes the developmental decision after requirement analysis and their critical evaluation. The plan of development is also an artifact considered during this research work. This design phase is key to success in the development and implementation steps. Furthermore, the completion of the design is responsible for proof of concept as successful completion and demonstration. The demonstration of the implementation of the proposed solution is necessary for the evaluation of the work regarding different parameters. The demonstration and evaluation phases result in outcomes logs for the comparison of this work with other considerable researches in the area and domain. The testing is a continuous process. During this phase, every step is performed and logs are recorded that give further insight into the requirement. This log also tells about, whether other objectives are met. Track of research leads to success in the case if proper design considerations are made. A design model is considered as fully effective and complete in all manners if it meets the requirements and objectives of the study. The effectiveness and completeness of the design are considered key to success in finding a proper solution to the problem.

3.4 Implementation and Evaluation

The proof of concept is evaluated for its effectiveness and performance measures. The results regarding data communication outcomes are collected and then analysed according to the objectives. The objectives are already mentioned at the start of this chapter. Performance is measured and the relevance of output is checked according to step 2 described in the design science research process. The processing time of the algorithm will be collected from the IoT environment and devices and will be considered as data for analysis. The processing time will be measured with a different resource. During every data transfer stage, data security will be analysed at the packet level. The processing time and security of data packet are two major factors that are to be analysed during this phase. The results will be based on the effectiveness and performance of the system after being implemented. The results may vary dependent on the technology and followed standards. If the design requirement is satisfied according to the used technology and security protocols then the evaluation of the proof of concept will be considered as successful. Also, the design should satisfy the identified problems and their secondary questions are well.

4. Results Discussion

Design consideration for the security solution already described in the previous chapter in detail. The planned design consists of the following three major components.

i. Class-0 IoT Devices
ii. Security Gateway to be used in IoT network
iii. Web Server

The role of these three components is described in this chapter with all aspects. The proposed solution is viewed in detail to check whether it fulfils the requirement or not. These requirements are described in the second phase of design.

i. Security of communicated data between source IoT devices and sink node
ii. Security of communicated data between sink node and Security Gateway

The final design is expected to satisfy the requirements mentioned in the above lines. The proof of concepts is based on the implementation of the designed solution which is considered as the foundation of the IoT security.

4.1 Data Security from Class 0 IoT Device to Security Gateway

An IoT device is taken as highly constrained devices when its RAM capacity is less than 10 Kilobytes and ROM capacity is less than 100kilo Bytes. This threshold level of resources enables devices to be called as class 0 IoT device. Such a device is Arduino Uno as it has only 2-kilo Bytes of ROM and 32kiloBytes of RAM. Its processing ability is 16MHZ. Arduino can collect the data from different sensors attached to it. This symmetric encryption can apply security at the data link layer. On the other hand, this security solution works in collaboration with IEEE standards like 802.11n, 802.15.4 or any other wireless standards. AES symmetric data encryption works with wireless nodes at the data link layer with other hardware tools as well. The data transfer strategy works according to the governing protocols. This data transfer is also dependent on the hardware being used. Both IEEE standards like 802.11n or 802.15.4 are used as wireless standards. These standards are also incompatible with LoWPAN or ZigBee used in wireless environments.
As the IoT device starts a session, these devices secure their communication using the Pre-shared key which is installed on every authorized IoT device. These devices communicated with the gateway using PSK. PSK is implemented on every device.

4.2 Data Security during the stay of data at the Security Gateway

Gateway hosts the security protocols that are used for security purposes for highly constrained devices. However, the problem arises when the resource needed by a protocol is much more than a class 0 IoT device has. The gateway performs as an intermediary that has enough resources to support the security protocols. Therefore, the security mechanism is implemented by a gateway that provides data security over the internet.

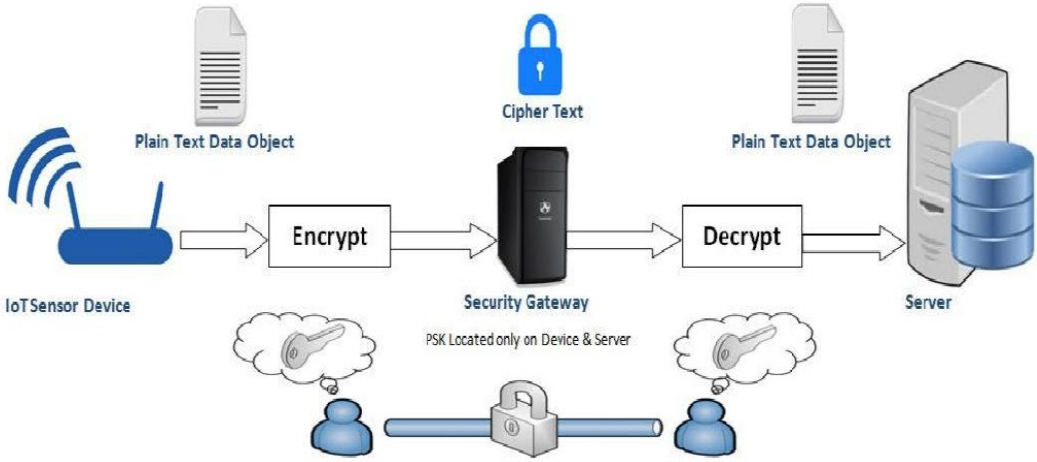

Figure 2. Encryption of Data Objects Zhang et. al. [9]

The devices send the data using HTTP and CoAP while the gateway uses TLS or HTTP for communication with the webserver. A packet that carries data has the overhead that contains information about it. This data packet follows a specific payload format that is converted into JSON objects and then encrypted using AES symmetric encryption. This is either 128 bit or 256 bit that is to be applied. Therefore this object of data is placed in the payload section of the transmitted data packet. This information is located in the packet header that also contains the addresses like destination and source nodes. These addresses are not encrypted and remain as they are the newly created JSON object is readable over the destination only and therefore it's not readable during gateway or any intermediary. Also if the web server sends any information to the sender IoT device or any other, this information is not readable by gateway because of its innate encryption using PSK.

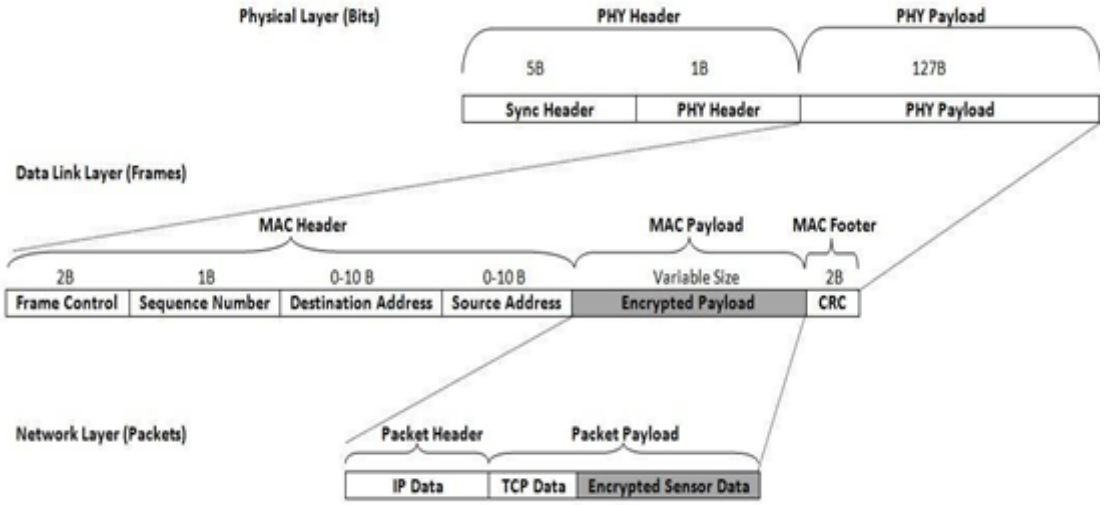

Figure 3. Security From Devices To Gateway Notra et. al. [3]

The figure 3 applies the security framework at the network layer and data link layer when the data is transferred to the security gateway. AES encryption is a hardware-based solution that is applied to the data link layer. The

information encryption is PSK based. The devices are authorized to use and read the information that has a hold over PSK. On the layer step, security measures take care of the contents of the data objects only. Addressing information of source and sink nodes are always not encrypted in this layer. The object of data is always encrypted using a symmetric key. This encrypted information is only shared with the server only as server is the destination. Therefore, it is not possible that any intermediary device can access or decrypt the data during the transmission phase.

4.3 Data Security when data is transferred from Gateway to Server

Security gateways are major devices that are rich in resources and can run operating systems and security protocols. This way secure communication is not compromised over the internet. The gateway acts as a small microcomputer. This Microcomputer runs the Linux operating system. Its model B of RPi comes with an Ethernet port with support of single-core CPU having 700 MHZ clock speed. It has support for SD card reader that can be used for onboard storage support and 512 RAM SDRAM. All of these exemplify these abilities to be viewed as 512 MB RAM. These resources are huge and have enough memory to run a security protocol as a super protocol.

The data transmission process from the server to IoT is depicted in figure 4 below. JSON format is being used for data object reading using the sensor. AES works with a key length of 128 bit for encryption that is applied before transmitted over the gateway using some wireless medium.

AES 128 bit PSK and WPA2 PSK is used for wireless communication medium security. The security is ensured as the known and authenticated devices have only access to PSK and transmission medium. Therefore, the transmission process is secured from attackers.

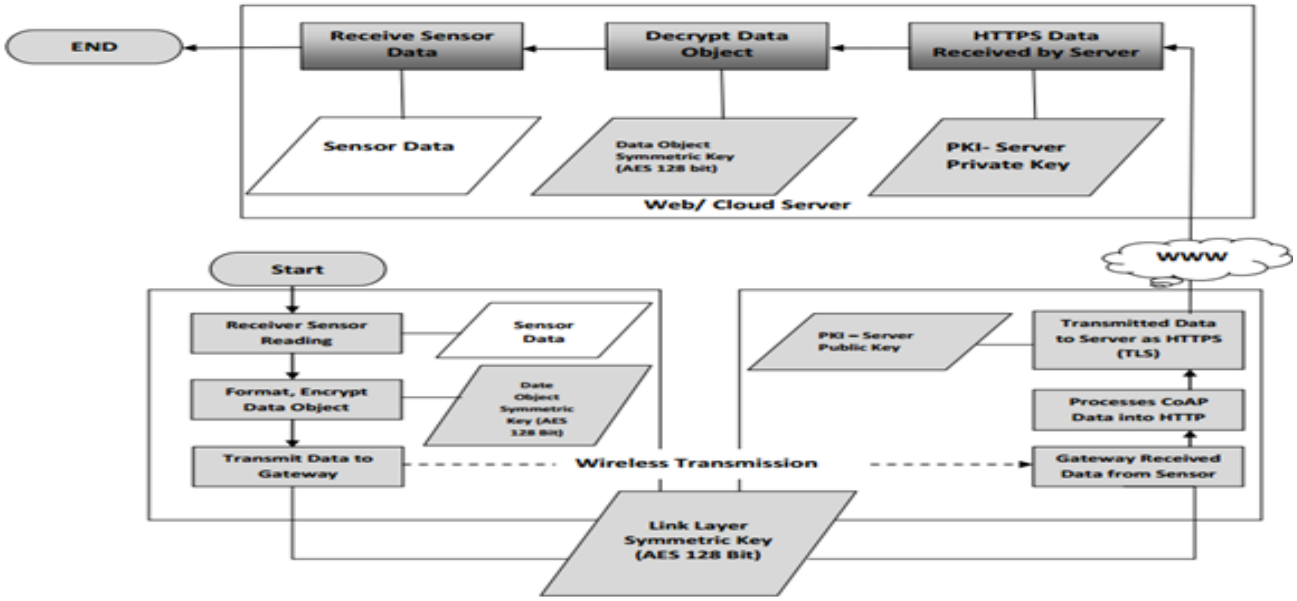

Figure 4. Device to Server, Solution Overflow

In IoT device microcontroller used as Arduino Uno and for connectivity Ethernet shield was used. Wireless shields could also be used but to directly connect the wireless router with a microcontroller with the help of Ethernet Cable. Proceeding of POC was ensured. Microcontroller is connected with the DHT11 sensor to read the data and format it into a JSON look.

IoT sensor and its functionality are shown in Figure 5 When the device gets connected it automatically starts data reading from the server. As long as the power source is connected from the device it will continue to perform this reading. And data reading will be stopped after the disconnection of power supply.

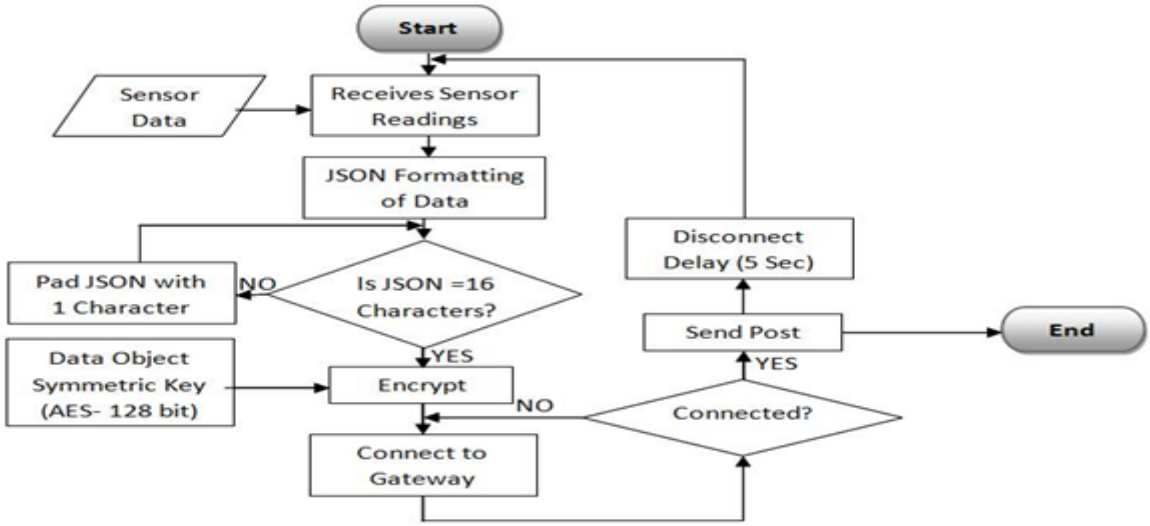

Figure 5. IoT Sensor Block Diagram

The process is used to format the sensor's data like its temperature. The padding process is required due to the requirement of fixed object size in AES. Data is encrypted using the symmetric key of 128 bit of AES encryption.

```
String data="{\"temp\":\"";
        data+=t;
        data+="\"}";
        while (data.length()<16 )
                {
                Data+="*";
                }
//Parsed JSON data. Pad data with "*" if less than 16 characters
//"t"= Temperature variable from sensor
Unit8_t key[]={'a' , 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p'};
//Declaration of AES 128 bit key
Data.toCharArray(dataEnc, sizeof(dataEnc));
//Conversion of JSON to Character array
 Aes128_enc_single(key,dataEnc);
//Encrypt with AES 128 bit single block cipher
Base64_encode(dataEncoded, dataEnc, 16);
//Encoding with base 64
```

Figure 6. Code in Arduino for Data Encryption, Encoding, and JSON Data Parsing

When client of the web tries to connect with Arduino Uno then it makes the client connection with the security gateway. After connection is being established then Arduino Uno uses the post method to send the data. Http is used for this communication. Before the transmission of this data post contents of HTTP are added in encrypted data. There is another alternative to use Coap for this purpose but it will make implementation heavier due to the extra suitable coding for the microcontroller and its extra configuration. Gateway sends an acknowledgment to the microcontroller after receiving the data which was sent through the POST method. The loop process is again restarted after waiting for the expected response.

0000	50	4f	53	54	20	2f	77	65	62	73	65	72	76	65	72	2f	POST/webserver/webclient.php HTTP/1.1
0010	77	65	62	63	6c	69	65	6e	74	2e	70	68	70	20	48	54	Host: 192.168.2.102
0020	54	50	2f	31	2e	31	0d	0a	48	6f	73	74	3a	20	31	39	Content-Type: text/plain
0030	32	2e	31	36	38	2e	32	2e	31	30	32	0d	0a	43	6f	6e	Content-Length:24
0040	74	65	6e	74	2e	54	79	70	65	3a	20	74	65	78	74	2f	
0050	70	6c	61	69	6d	0d	0a	43	6f	6e	74	65	6e	74	2d	4c	KHnhbvpoersw=kmnzLpegZC=
0060	65	6e	67	74	68	3a	20	32	34	0d	0a	0d	0a	5a	47	69	
0070	6f	46	7a	6f	41	70	46	6b	39	43	66	56	39	58	46	51	
0080	68	78	51	3d	3d												

Figure 7. TCP Captured Packet from Attached Sensor Device

4.4 IoT security Gateway

Figure 8 IoT gateway is built using the Raspberry Pi model. Its microcontroller is very resourceful and is very suitable for heavy algorithms due to the intensive nature of resources. IoT devices that were highly constrained do not support mechanisms that can work easily on this model. This model contains RAM of 512 MB AND CPU of 700 MHZ with an extendable storage card. SD Card of 8 GB is sufficient for this purpose. Its working can easily be embedded with Linux OS.

The specialized version of Linux known as Raspbian version is used as a security gateway for IoT devices [13]. Wireless router is connected with device using a wireless USB adapter. WPA2 64 byte AES symmetric key encryption is used to provide security to the wireless network.

Figure 8. IoT Security Gateway

4.5 Web Server

The laptop was used for the configuration of the server using LAN for Proof of Concept. Filtration of data for data transmission is the responsibility of this machine. SSL Certificate is used for the configuration of an Apache Web server. For receiving of HTTPS connection is used by TLS/SSL server.

POST is sent by the gateway to the server after a connection is being established. Encrypted sensor data is contained by this POST. The online server's web service processing is shown in Figure 9.

This data is sensed and encrypted using a base 64 encoding method. The data is extracted by web service and retrieved from the payload. Further, this data is decoded and it comes back to its original form. For this purpose, the data is decoded using a decrypting algorithm. The decoded data is converted to JSON format. This JSON format data is stored in the database. This demonstration is also displayed on the webpage. The results are also accounted for from the sensor inputs and further stored in the database.

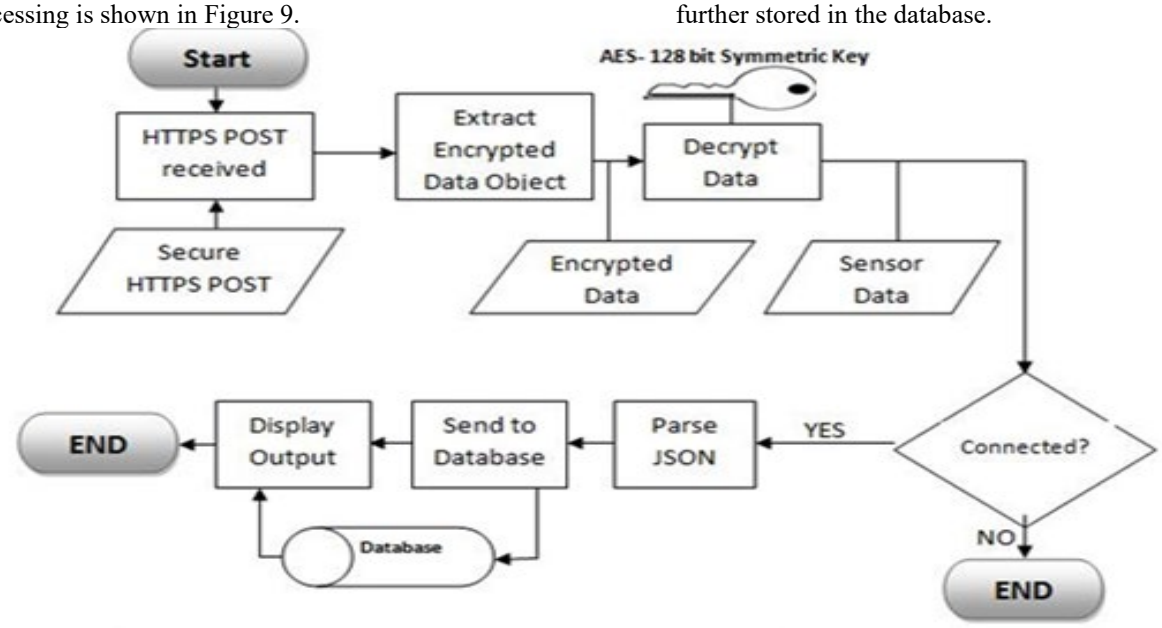

Figure 9. Block Diagram of Web Server

The above-given figure shows the process of decryption that is handled by the web service. This process starts with a symmetric key and cipher text. This working data is necessary to decode the information. The data is decoded from the base 32 encoded form. In Figure 10 a reference to AES 128 bit cipher is "RJINDAEL-128". This reference is used to process the decoded data. The decrypted outcome is further parsed maintained for other processing as well. Then this parsed data is sent to a database using the upload method. Tag "original message" is stored with the decoded data when it is stored. The date is also attached as the time stamp.

```
function decrypt_data ($data, $iv, $key) {
        $cypher = mcrypt_module_open('rijndael-128', '', 'ecb', '');
        if (is_null ($iv)) {
                $iv = mcrypt_create_iv (mcrypt_enc_get_iv_size ($cypher), MCRYPT_RAND);
                }
        // initialize encryption handler
        if (mcrypt_generic_init ($cypher, $key, $iv)! = -1) {
                // decrypt
                $decrypted = mdecrypt_generic ($cypher, $data);
                mcrypt_generic_deinit ($cypher);
                mcrypt_module_close($cypher);
                return $decrypted;
                }
                return false;
}
if ($ctext != NULL) {
        $res = decrypt_data (base64_decode ($ctext), null, $key);
        }
else

        {

        echo "No data received \n";

        }
```

Figure 10. AES 128 Bit Cipher

4.6 Evaluation of the System

The proposed system is evaluated for its ability that it meets the targeted abilities or not. These performance factors are compared with their expected performance as mentioned. In this step, the objectives were defined for the problems mentioned. The table below describes the requirements and their associated with the problems.

During the research evaluation, the time complexity and data losses are also measured for its evaluation. The consistency of the system is also checked when it is implemented for highly constrained class 0 IoT devices.

Table 3. Consideration for System Evaluation

Problem Serial No	Description of the Problem	Objectives Targeted
1	Highly constrained IoT devices cannot communicate in a secure manner	1- Security of data when it is communicated between IoT devices and destination node.
		2- Time efficiency and data loss efficiency.
1.1	IoT devices can communicate with web service but in an insecure manner.	1- Security of data when it is communicated between the IoT devices and web server.
		2- Security of Data security when it is transmitted between server and gateway.

Objective 1 is generally described and it implements able to the entire solution manual. To ensure data confidentiality while the data is transferred from source to sink and authenticity and integrity during the data transfer from the IoT Device to the security gateway, each objective is clear. The fulfillment of these objectives is dependent on the encryption mechanism at the DLL and the object as well. The encryption process is symmetric that uses data from the source devices at the initial stage of data processing. AES 256 bit along with WPA 2 ensure

the data security of communication from IoT devices to the gateway. The encryption mechanism can be changed with the change of technology of transmission.
More resources are needed for this purpose of encryption. The objective no 5 can be fulfilled in the proposed solution it the system resources are affected at a very low level. The solution should be less resource demanding. Arduino Uno demands 16kilo byes of Ram and 0.5 kilobytes of ROM for its basic processing. This way the used RAM is half of the available. Because the RAM is 32 KB in total in Arduino. While the ROM needed is 28% of the total available. The demand for the resources increases when the encryption process added in it. For AES 128 bit process, additional 0.47KB ROM is needed with 0.5RAM other than the initially needed resources. The minimum resources of Arduino Uno are less than 100 KB of ROM. Therefore, the minimum resources available with Arduino are in line with the demand for resources. A total time of 0.46 sec is needed to process the encryption procedure. This encryption is performed when the data from a sensor input is passing on the Arduino. This additional overhead is 0.47 Kb of Rom and 0.5 Kb of RAM other than the basic application needs of the Arduino. However, more efficient configurations of the Arduino device can lead to more time efficiency in its operations. Other factors that lead to time efficiency may include the protocols, configurations, and algorithms that reduce the requirements as well.

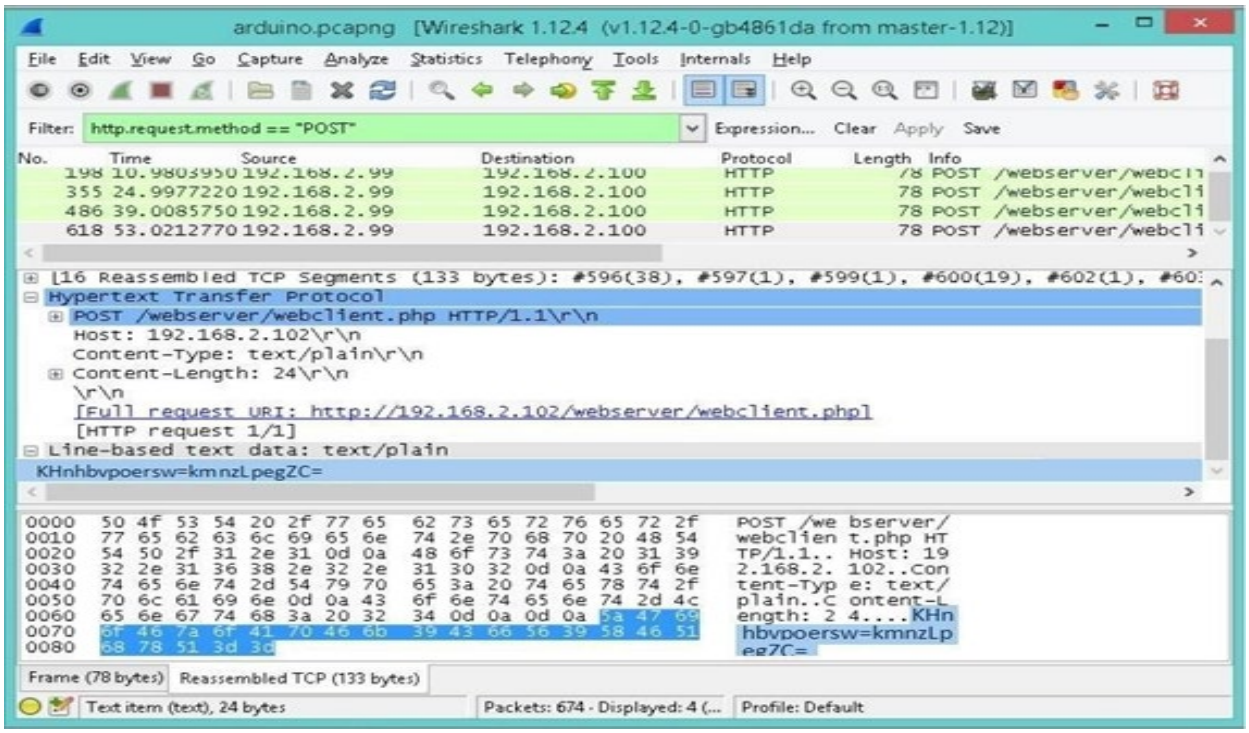

Figure 11. Captured Packet from IoT Post

A data packet is transmitted from the IoT device. This process is shown in figure 11. The highlighted data of the POST is encrypted in the original. Header information is given in text format and not in an encrypted format. In case some attacker attacks the device, he may have to access the network first. If he accesses the network, he then needs to access the gateway before it accesses the data node. Data objects are encrypted therefore, the hacker cannot be able to read the encrypted data. Therefore, it can be said that the encryption of data objects fulfils the following objectives.

Objective 1: Security of transmitted Data when data is transmitted between IoT device and sink
Objective 3: security of transmitted data when it is communicated from gateway to IoT device

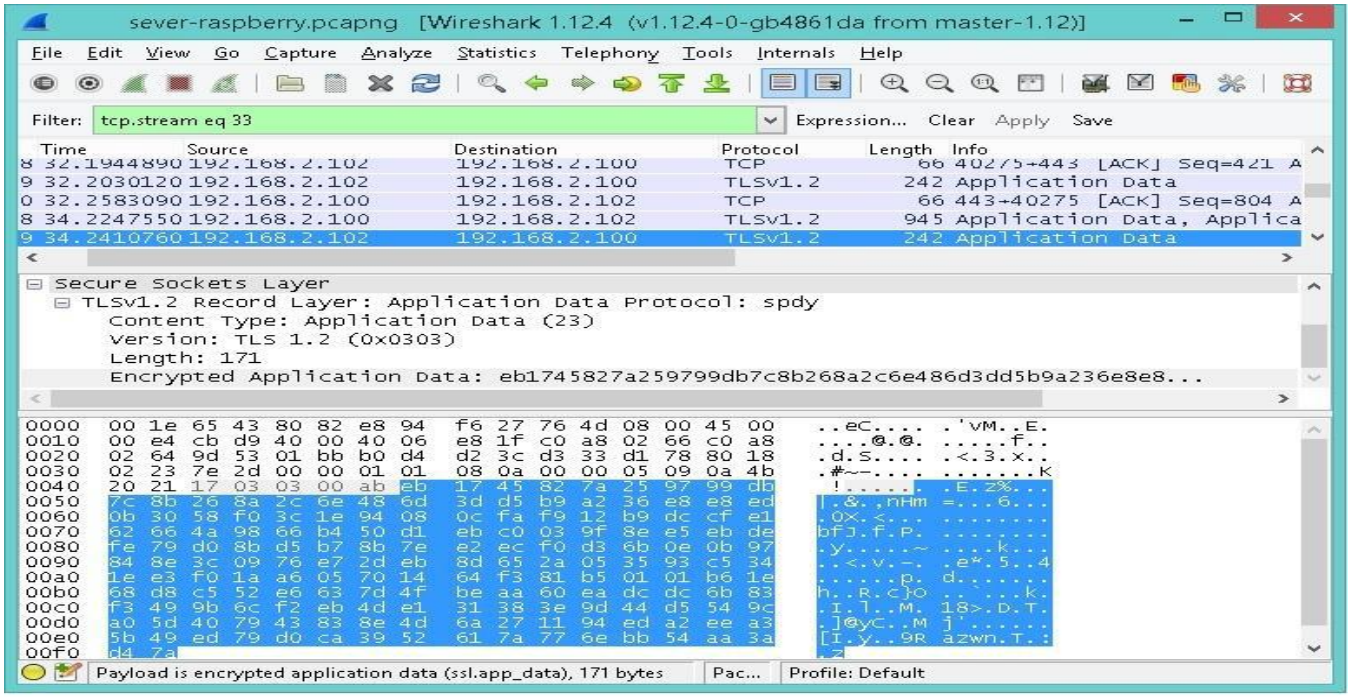

Figure 12. Captured TLS Packet from Web Server

Data is converted according to HTTPS with RSA using a 2048 bit session key when the data reaches the gateway. After this encryption, the data is forwarded to the webserver. This process is shown in figure 12 Application of encrypted application is shown when the encrypted data is received by an online server. During this demo, Wireshark is used as a tester of the protocol. This protocol analyzer helps in analyzing the data analysis and exchange of traffic to know about the behavior of the traffic on a link. In this demonstration, this is used for traffic behavior analysis between the online server and gateway. The data is encrypted and then sent to the server therefore it is not readable by any device. However, the authorized nodes that have the keys for decryption purposes can decrypt the data. Therefore, the objectives achieved here include 1 & 2.

Obj 1: Security of data when it is transmitted between constrained IoT devices and sink.
Obj 2: Security of data when it is transmitted between destinations to the gateway

The authenticity of data is dependent on the use of asymmetric encryption. The key is also securely communicated with this method. The symmetric key encryption method also allows for updating the key automatically. There is a chance that the encryption key is compromised, and then a simultaneous update is needed on all devices. This updating process is dependent on the manager of the encryption process who is looking after the whole encryption and decryption procedure. This key processing can be taken as a future part of this research for highly constrained IoT devices. This proposed solution-focused on the lower power IoT devices. This algorithm ensures the authenticity of the data at both the sender and receiver end. Both of them need a key to process the data at the earliest. Additional functions may be incorporated at this place however more resources will be needed for this purpose. The extra need for storage will be faced if the private key is to be stored. Key size of the private key reaches up to 1.2 Kb. Limited resources of IoT device restrains the devices to perform this storage operation. Therefore and extra SD card is needed for this purpose.

This protocol is HTTPS (TLS). When the data is communicated securely, then there remains a gap in the physical security of the devices. However, this is not is the scope of this article. Our focus lies in communication security. The shared keys are produced during the AES encryption which is stored by the devices. If these devices are accessed physically then security is compromised as unauthorized persons can read the data using this key. However, we assume that the environment is physically secure and no one can access the devices physically. And hence the keys are securely stored in the devices.

This solution can be made more effective using a broader range of updates and after some customizations. All these devices need a mechanism to be implemented after testing their integration with gateway communication. In case all the devices lie in an individual LAN, their testing scenario needs to be one to one communication. And in case devices lie in WAN or more than one LAN then many gateways can also be used using the proposed method. Security measures like SSL, remote connectivity of devices are also feasible with more than one gateway. In this way, the testing scenario includes one to one

communication and many to many communications as well.

5. Conclusion

This research is concentrating on the security of information correspondence of profoundly obliged gadgets and the web and their middle of the road gadgets. Exceptionally obliged gadgets are running shy of assets and don't be able to help the TLS/DTLS conventions for the safe correspondence. Various holes in the existing arrangement has been recognized and attempted to be tended to in this examination utilizing and rebuilding of pre-characterized techniques. Entranceway itself cannot examine the transmitted information sent from IoT appliance as this can be seen because of the difficult information and is encoded exploitation AES cryptography. Entrance last transmits it to the online employing a checked web show HTTPS (TLS). Past the degree of this investigation, this can be basic to form a solid course of action of physical security of the particular contraptions. because the traditional key of AES regular cryptography is being inspired by the contraptions, of specific devices is gotten to physically the shared key is often undermined and any

Hashing calculations are ideal to use to maintain a strategic distance from such sort of assaults. To trade the key among various gadgets and to guarantee the genuineness of information deviated encryption is utilized. If there should be an occurrence of spillage of security key all gadgets may refresh their key. Uneven cryptography is never suggested for mass information transmission yet here utilizing distinctive displaying it is demonstrated this is conceivable to structure a mass information trade system utilizing awry encryption process on less asset gadgets. On the off chance that we utilize RESTful API gadgets to become ready to convey utilizing web administrations. If there should be an occurrence of spillage of key hilter kilter cryptography let u update the key, and this transmission is additionally held utilizing RESTful API's strategy.

Conflicts of Interest:

The authors declare that there are no conflicts of interest regarding the publication of this article.

References

[1] Kumar, J. S., & Patel, D. R. (2014). A survey on internet of things: Security and privacy issues. International Journal of Computer Applications, 90(11).

[2] Xu, Q., Ren, P., Song, H., & Du, Q. (2016). Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations. IEEE Access, 4, 2840-2853.

[3] Notra, S., Siddiqi, M., Gharakheili, H. H., Sivaraman, V., & Boreli, R. (2014, October). An experimental study of security and privacy risks with emerging household appliances. In 2014 IEEE conference on communications and network security (pp. 79-84). IEEE.

[4] Bormann, C., Castellani, A. P., & Shelby, Z. (2012). Coap: An application protocol for billions of tiny internet nodes. IEEE Internet Computing, 16(2), 62-67.

[5] Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015, June). Security and privacy challenges in industrial internet of things. In 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC) (pp. 1-6). IEEE.

[6] Dave, B., Kubler, S., Främling, K., & Koskela, L. (2016). Opportunities for enhanced lean construction management using Internet of Things standards. Automation in construction, 61, 86-97.

[7] Hernandez-Ramos, J. L., Pawlowski, M. P., Jara, A. J., Skarmeta, A. F., & Ladid, L. (2015). Toward a lightweight authentication and authorization framework for smart objects. IEEE Journal on Selected Areas in Communications, 33(4), 690-702.

[8] Hu, Z. (2011, August). The research of several key question of internet of things. In 2011 International Conference on Intelligence Science and Information Engineering (pp. 362-365). IEEE.

[9] Zhang, L., Zhou, F., Mislove, A., & Sundaram, R. (2013, April). Maygh: Building a CDN from client web browsers. In Proceedings of the 8th ACM European Conference on Computer Systems (pp. 281-294).

[10] Hussain, S., Abbas, S., Sohail, T., Adnan Khan, M., & Athar, A. (2019). Estimating virtual trust of cognitive agents using multi layered socio-fuzzy inference system. Journal of Intelligent & Fuzzy Systems, 37(2), 2769-2784.

[11] Areej Fatima, Muhammad Adnan Khan, Sagheer Abbas, Muhammad Waqas, Leena Anum, and Muhammad Asif, Evaluation of Planet Factors of Smart City through Multi-layer Fuzzy Logic (MFL). The ISC Int'l Journal of Information Security. 51-58, 2019.

[12] Siddiqui, S. Y., Hussnain, S. A., Siddiqui, A. H., Ghufran, R., Khan, M. S., Irshad, M. S., & Khan, A. H. (2019). Diagnosis of Arthritis Using Adaptive Hierarchical Mamdani Fuzzy Type-1 Expert System. EAI Endorsed Transactions on Scalable Information Systems, 19(18), 1-16.

[13] Atta, A., Abbas, S., Khan, M. A., Ahmed, G., & Farooq, U. (2018). An adaptive approach: Smart traffic congestion control system. Journal of King Saud University-Computer and Information Sciences.

[14] Khan, M. A., Umair, M., Saleem, M. A., Ali, M. N., & Abbas, S. (2019). CDE using improved opposite based swarm optimization for MIMO systems. Journal of Intelligent & Fuzzy Systems, 37(1), 687-692.

[15] Khan, M. A., Umair, M., & Choudhry, M. A. S. (2015). GA based adaptive receiver for MC-CDMA system. Turkish Journal of Electrical Engineering & Computer Sciences, 23(Sup. 1), 2267-2277.

[16] Khan, M. A., Umair, M., & Choudry, M. A. S. (2015, December). Island differential evolution based adaptive receiver for MC-CDMA system. In 2015 International Conference on Information and Communication Technologies (ICICT) (pp. 1-6). IEEE.

[17] Ali, M. N., Khan, M. A., Adeel, M., & Amir, M. (2016). Genetic Algorithm based adaptive Receiver for MC-CDMA system with variation in Mutation Operator. International Journal of Computer Science and Information Security, 14(9), 296.

[18] Umair, M., Khan, M. A., & Choudry, M. A. S. (2015, December). Island genetic algorithm based MUD for MC-CDMA system. In 2015 International Conference on Information and Communication Technologies (ICICT) (pp. 1-6). IEEE.

[19] Umair, M., Khan, M. A., & Choudry, M. A. S. (2013, January). GA backing to STBC based MC-CDMA systems. In 2013 4th International Conference on Intelligent Systems, Modelling and Simulation (pp. 503-506). IEEE.

[20] Kashif, I., Muhammad, A.K., Sagheer, A., Zahid, H., & Areej, F (2018). Intelligent Transportation System (ITS) for Smart-cities using Mamdani Fuzzy Inference System, International Journal of Advanced Computer Science and Applications (IJACSA). ISSN: 2158-107X, Vol. 9, No. 2, (pp. 94-105), Digital Object Identifier (DOI): 10.14569/IJACSA.2018.090215.

[21] Abbas, S., Khan, M. A., Ata, A., Ahmad, G., Saeed, A., & Anwar, N. (2019). MULTI USER DETECTION USING FUZZY LOGIC EMPOWERED ADAPTIVE BACK PROPAGATION NEURAL NETWORK. Neural Network World, 29(6), 381-401.

[22] AsadUllah, M., Khan, M. A., Abbas, S., Athar, A., Raza, S. S., & Ahmad, G. (2018). Blind channel and data estimation using fuzzy logic-empowered opposite learning-based mutant particle swarm optimization. Computational intelligence and neuroscience, 2018.

[23] Khan, M. A., Umair, M., & Choudry, M. A. S. (2015, December). Island differential evolution based adaptive receiver for MC-CDMA system. In 2015 International Conference on Information and Communication Technologies (ICICT) (pp. 1-6). IEEE.

[24] Ata, A., Khan, M. A., Abbas, S., Ahmad, G., & Fatima, A. (2019). MODELLING SMART ROAD TRAFFIC CONGESTION CONTROL SYSTEM USING MACHINE LEARNING TECHNIQUES. Neural Network World, 29(2), 99-110.

[25] Siddiqui, S. Y., Athar, A., Khan, M. A., Abbas, S., Saeed, Y., Khan, M. F., & Hussain, M. (2020). Modelling, Simulation and Optimization of Diagnosis Cardiovascular Disease Using Computational Intelligence Approaches. Journal of Medical Imaging and Health Informatics, 10(5), 1005-1022.

[26] Siddiqui, S. Y., Khan, M. A., Abbas, S., & Khan, F. (2020). Smart Occupancy Detection for Road Traffic Parking using Deep Extreme Learning Machine. Journal of King Saud University-Computer and Information Sciences.

[27] Hussain, A., Hussnain, S. A., Fatima, A., Siddiqui, S. Y., Saeed, A., Saeed, Y& Khan, M. A. (2020). A Novel Approach for Thyroid Disease Identification Empowered with Fuzzy Logic. IJCSNS, 20(1), 173.

[28] Naz, N. S., Khan, M. A., Abbas, S., Ather, A., & Saqib, S. (2020). Intelligent routing between capsules empowered with deep extreme machine learning technique. SN Applied Sciences, 2(1), 108.

[29] Farooq, M. S., Khan, M. A., Abbas, S., Athar, A., Ali, N., & Hassan, A. (2019, November). Skin Detection based Pornography Filtering using Adaptive Back Propagation Neural Network. In 2019 8th International Conference on Information and Communication Technologies (ICICT) (pp. 106-112). IEEE.

[30] Ahmad, G., Khan, M. A., Abbas, S., Athar, A., Khan, B. S., & Aslam, M. S. (2019). Automated diagnosis of hepatitis b using multilayer mamdani fuzzy inference system. Journal of healthcare engineering, 2019.

[31] Umair, M., Khan, M. A., & Saleem, M. A. (2016). Piranha fish optimization for multi user detection in OFDMA system. International Journal of Advanced And Applied Sciences, 3(6), 35-40.

[32] Khan, M. A. (2016). MULTIUSER DETECTION USING COMPUTATIONAL INTELLIGENCE IN MULTI-CARRIER COMMUNICATION SYSTEMS (Doctoral dissertation, Isra University, Hyderabad, Sindh).

[33] Iqbal, N., Abbas, S., Khan, M. A., Alyas, T., Fatima, A., & Ahmad, A. (2019). An RGB Image Cipher Using Chaotic Systems, 15-Puzzle Problem and DNA Computing. IEEE Access, 7, 174051-174071.

[34] Tan, L., & Wang, N. (2010, August). Future internet: The internet of things. In 2010 3rd international conference on advanced computer theory and engineering (ICACTE) (Vol. 5, pp. V5-376). IEEE.

[35] Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of management information systems, 24(3), 45-77.

[36] Kortuem, G., Kawsar, F., Sundramoorthy, V., & Fitton, D. (2009). Smart objects as building blocks for the internet of things. IEEE Internet Computing, 14(1), 44-51.

[37] Alawatugoda, J., Jayasinghe, D., & Ragel, R. (2011, August). Countermeasures against Bernstein's remote cache timing attack. In 2011 6th International Conference on Industrial and Information Systems (pp. 43-48). IEEE.