International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 7 Issue 5, May - 2017,
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 Impact Factor: 6.505 | Thomson Reuters Researcher ID: L-5236-2015

ANALYZING THE SECURITY MECHANISM FOR RESOURCE-CONSTRAINED IoT DEVICES

Nutan Sharma[1], Dr. Kalpana Midha[2]

Department of Computer Science

[1,2]OPJS University, Churu (Rajasthan) – India

Abstract

The appearance of cheap embedded computing devices capable of wireless communications is leading to the emergence of an Internet of Things (IoT). The ability to network embedded devices opens up opportunities to develop new applications. The embedded computing devices deployed within the Internet of Things (IoT) are expected to be resource constrained. This resource constraint not only applies to memory and processing capabilities, but the low-power radio standards utilized further constrain the network interfaces. The IPv6 protocol provides a suitable basis for interoperability in the IoT, due to its large address space and a number of existing protocols that function over IP and its flexibility. We investigate how existing IP based network management protocols can be implemented on resource constrained devices. We present the security mechanism for resource-constrained IoT devices.

1. INTRODUCTION

As of late, the Internet of Things (IoT), authored all things considered in 1999, has turned into a developing worldview in wireless communications. IoT is currently an intriguing issue in Information and Communication Technology (ICT) and has drawn the consideration of many research organizations. The nonexclusive infrastructure of IoT is a network of devices or objects, for example, implanted computers, controllable and intelligent automated devices, sensors, and Radio Frequency Identification (RFID) labels, notwithstanding the IoT gateway and the remote server. IoT devices can associate and trade data with different devices and services over a network and over the worldwide Internet. The organizations of IoT center technology incorporate home automation, manufacturing, ecological observing, and medical and healthcare systems. A future super market is foreseen for a wide extent of applications that use IoT devices and technology.

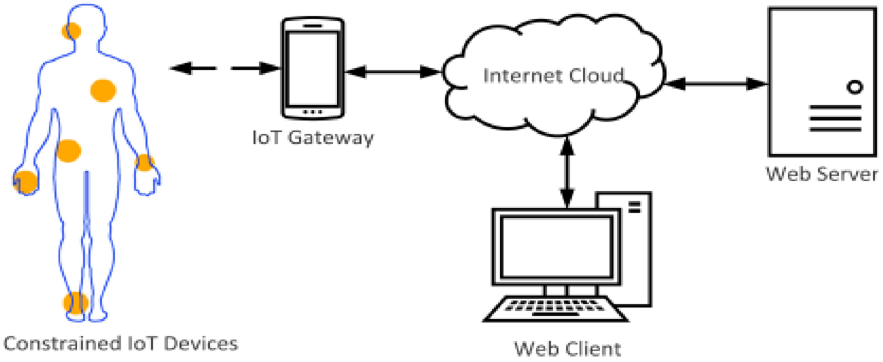

Figure 1: A generic IoT system using the example of resource-constrained IoT medical devices

The constrained IoT devices, Class-0 IoT devices, will be devices with restricted or constrained resources concerning CPU preparing power, ROM, RAM, and battery life. In any case, these devices still have the ability of giving their planned functionalities. The constrained IoT devices are often little in size with restricted functions, for example, sensors and smart devices controlling electrical appliances or services. They are fit for gathering and transmitting data, for example, sensor readings, over the Internet for capacity and analysis. The gathered and transmitted data might be personal, private, and delicate.

1.1 Preliminaries

As a far reaching arrangement that expects to secure the data way through all the IoT system segments represented in Figure 2 Moreover, the vast majority of the accessible arrangements don't target Class-0 devices. A security mechanism like that created by DoukasetIoT technology has created as of late to incorporate an ever increasing number of devices embracing implanted systems and communication interfaces. The future development of IoT deployments involves healthcare, instruction, manufacturing, and transportation. The fundamental idea driving IoT devices is the likelihood of gathering and sending data over the Internet. The architecture of the IoT segments can be partitioned into three layers: the perception layer (physical devices), network layer (transmission layer), and application layer. Nonetheless, each layer has its very own security needs. This paper centers around the perception layer for verifying the whole data way. Figure 4.9 represents the layered architecture of IoT parts and the data network.

Constrained IoT devices can be grouped dependent on the accessible resources into three classifications: Class-0 (C0), Class-1 (C1), and Class-2 (C2) devices. A correlation of the accessible resources in each class is appeared Table 1. It is evident that the Class-0 devices have many less resources in terms of RAM and ROM recollections. Moreover, the accessible RAM estimate can't handle serious security mechanisms. IoT security needs to cover the whole IoT hierarchal architecture. IoT security traverses the application layer, network layer, and perception layer. The essential security concerns incorporate data privacy, respectability, and accessibility. Constrained IoT devices have restricted resources and consequently are constrained to the protocols and standards they can bolster. Endeavors have been made by groups, for example, the Internet Engineering Task Force (IETF) to create protocols and standards progressively appropriate for constrained situations, for example, Datagram Transport Layer Security (DTLS) and Constrained Application Protocol (CoAP), by expanding the productivity and limiting the required registering resources.

The security of the transport layer for Class-1 and Class2 IoT devices can be accomplished utilizing DTLS over HTTP or CoAP. DTLS is an adjustment of the TLS protocol and has an overwhelming resource footprint notwithstanding existing application code in the device itself. Like HTTP, CoAP as a stand-alone protocol does not contain security highlights essential for secure data communication. So as to fix this issue, a variety of TLS was created to keep running under CoAP and over UDP called (DTLS). DTLS contains numerous highlights of TLS, for example, data encryption and verification, with added highlights to manage the lack of quality of UDP. As of late, CoAP over DTLS has been termed as CoAPS. In spite of the endeavors of the IETF group, there is as yet a scope of devices that miss the mark regarding the insignificant resources expected to help such advances over existing applications. These devices are known as "Class-0" as they miss the mark regarding the base edge (10 KB of RAM and 100 KB of ROM) to help secure communication utilizing TLS-based arrangements.

The negligible code size and memory utilization for utilizing DTLS were presented by Kumar et al. in the DTLS usage control. The memory necessities laid out in the report recommend that the base resource prerequisites for DTLS (3.9 KB of RAM and 15.15 KB of ROM) would not be doable in many Class-0 devices. It might likewise perform ineffectively on some Class-1 devices with association times as slow as 24 seconds for a secure transmission. As an end, an elective security arrangement is required for exceptionally constrained IoT devices, especially for Class-0 IoT devices.

2. A DISTRIBUTED SECURITY MECHANISM

This segment centers on the theoretical plan of a distributed security mechanism. The structure covers three IoT systems segments: the IoT device, IoT gateway, and remote web server. Every segment is talked about in detail alongside a portrayal of how the data are conveyed. The structure of the proposed security mechanism expects to accomplish the prerequisites for Class-0 devices that are reported in Table 1. The proposed arrangement secures data communication in Class-0-constrained devices by applying a 128-piece symmetric encryption (AES-128) to data objects, for example, sensor readings, before they are transmitted between the device and the gateway. The data are designed in JavaScript Object Notation (JSON) and are sent as a CoAP or HTTP POST to the gateway. The data object is scrambled utilizing a mystery key and must be decoded by devices with a similar key. This key is imparted to the goal, for this situation, the web server.

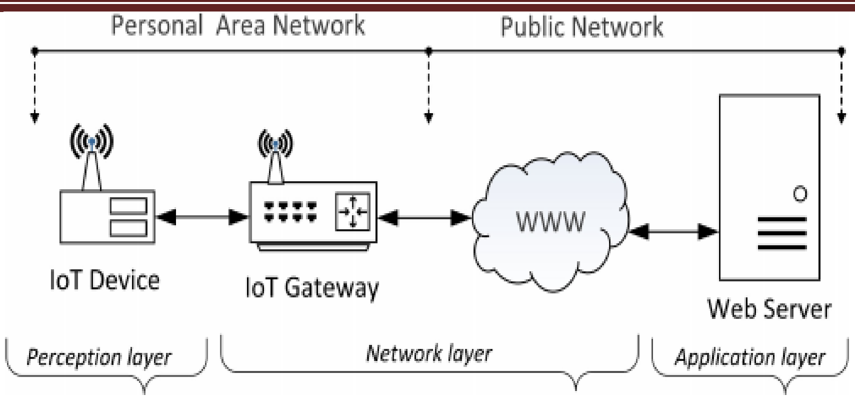

Figure 2: The three main layers of the layered architecture of IoT components.

Table 1: A comparison of some available security solutions for IoT devices

The concept	The drawback for class -0 devices
Enabling data protection through PKI encryption	Does not secure the device to the gateway
Datagram Transport Layer Security V1.2	Very heavy resource requirements
Object Security Architecture for the IoT	Very heavy resource requirements

Table 2: The design requirements for the proposed distributed security mechanism

#1	Provide data security between the Class-0 device and the IoT gateway
#2	Secure data transported between the IoT gateway and the Internet
#3	Perform efficiently with minimal resource consumption

Wireless transmissions in the LAN/PAN between the device and the gateway are secured at the Data Link Layer utilizing a wireless interface module. Constrained wireless standards, for example, IEEE 802.15.4 and protocols, for example, Low power Wireless Personal Area Network (6LoWPAN) are equipped for supporting AES 128-piece symmetric encryption at this layer. By utilizing an offered Pre-Shared Key (PSK) to scramble wireless transmissions, just approved devices associated with the network can get traffic. By encoding data objects at the device level (perception layer), just the device and the last goal will almost certainly read the scrambled data. An outline of the proposed security mechanism is represented in Figure 4.10. Further depictions of the proposed distributed security mechanism on each IoT system segment are given in the following passages.

3. DEVICE-TO-GATEWAY SECURITY

From the communication standpoint, another dimension of security between the IoT device and the gateway can be accomplished utilizing equipment based symmetric encryption of the Data Link Layer (DLL) as a feature of the wireless protocol (e.g., IEEE 802.15.4, IEEE 802.11n). Wireless transmission can be given utilizing an IEEE 802.15.4 module, for example, a ZigBee or 6LoWPAN interface. When associating with a network, devices are secured with a PSK, which is introduced on each approved device, and it is required for communication inception between the gateway and the constrained devices in the network. Any unapproved devices checking the traffic won't almost certainly decrypt data without the right PSK. Notwithstanding, the implicit wireless security shields data from substances without the PSK, leaves data uncovered in the event that somebody figures out how to bargain the wireless security, or capture the PSK from another device or from the gateway.

Privacy is guaranteed between the IoT device and the goal by encoding data at the object level. Object layer security exists at the application layer inside the payload of a transmission parcel. Objects in this setting allude to a compartment of data, which has been arranged to be intelligible. Various data positions exist for the web, including JSON, XML, and YAML. It is important that object-layer security applies cryptography to a data object, yet the header data, for example, the source and goal addresses stay uncovered. The parcel organization and data encryption are appeared in Figure 2.10. This dimension of encryption is utilized as a primary layer of protection, and it very well may be joined with the offered wireless security for more grounded security between the IoT device and the IoT gateway. It fills in as a second protective divider if there should be an occurrence of a traded off wireless network

Figure 4 portrays the two layers of security connected to data transmitted from the device to the gateway. Security is connected at the Data Link layer as equipment based AES encryption secured with a PSK. The second layer of security is connected just to the substance of the data object. Addressing and source data remain decoded in this layer. The data object is scrambled with a symmetric key, which has just been shared with the server so no intermediaries will almost certainly decrypt the data.

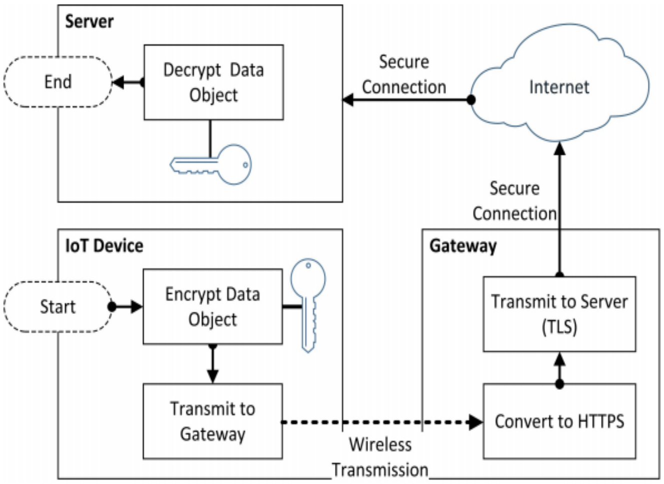

Figure 3: An overview of the proposed security mechanism shows the major processes that run on each component.

IoT gateways are computational devices with enough resources to run operating systems and protocols important to securely exchange traffic over the Internet. An IoT gateway may appear as a microcomputer with a Linux-based operating system. The gateway has adequate resource to apply substantial security and communication protocols that can't be bolstered by Class-0 devices. When data are gotten by the gateway, they are handled into HTTPS and arranged for transmission to the remote server. The gateway is designed with Secure Socket Layer (SSL) devices, which are utilized to make a secure HTTPS association between the gateway and the server. From the gateway point, one can advance secure communications to the server over the Internet utilizing the designed secure socket layer. The gateway goes about as an intermediary with adequate resources to help these security measures and secure data before sending it over the Internet. Data sent from the IoT device will be sent to the gateway utilizing protocols, for example, CoAP and HTTP and sent over the Internet utilizing HTTPS (HTTP over TLS) to the web server. In the proposed security mechanism, the payload of the packets is arranged as a JSON object and scrambled utilizing AES 128-piece or 256-piece symmetric encryption. This data object will exist inside the transmission payload, while the parcel header data, for example, source and goal address remains decoded, as showed in Figure 3.

4. WEB SERVER SECURITY

The messages being transmitted to the server are scrambled with the server's public key, which is introduced in the gateway. Just the server can decrypt messages utilizing its relating private key. The private key is situated on the server and isn't shared with some other devices. The definite flowchart of the proposed security mechanism with every single consecutive procedure that is mapped to the three IoT system parts is appeared in Figure 4.11.

When the HTTPS packets are gotten by the server, they are decrypted utilizing the private key. The scrambled data object would then be able to be decrypted utilizing the symmetric mystery key from the starting device, for this situation, our class-0 IoT device. On the off chance that the key is just present on one IoT device and the server, it tends to be utilized to confirm data got from either party. On the off chance that the key is shared with different devices, the devices are confirmed as a component of a group. This situation keeps up the classification of IoT data at whatever point it ignores a public network.

5. ADVANCED ENCRYPTION STANDARD

Advanced Encryption Standard (AES) is one such symmetric standard, which works at quick speeds and requires fewer resources than DTLS, making it entirely reasonable for Class-0 devices. AES can be effectively actualized and upgraded on hardware. AES inputs data as 16-byte (128-piece) hinders that are then encoded utilizing a cryptographic key that is 128 bits, 192 bits, or 256 bits in size. The bigger the key size, the more prominent the security and resource necessity for the device to scramble and decrypt Symmetric encryption can be connected at various layers of the communication stack, for example, the data link layer (e.g., wireless transmissions) and to explicit objects of data inside a message, for example, sensor readings. AES is appropriate for the necessities of Class-0 IoT devices in terms of the encryption speed and the required resources.

Symmetric cryptography includes scrambling data with a single encryption key, which is shared between various devices. Any device that has the key can decrypt data that have been encoded with a similar key. At the point when the key is shared with different devices, there is a higher hazard that it might fall into the wrong hands, and along these lines, it must be remained careful. As of now, in the proposed arrangement, the IoT data are scrambled in the IoT device utilizing a symmetric key. The symmetric key is static and is introduced just on the IoT device and the server. In this way, the gateway can't decrypt the parcel payload. Messages being transmitted from the gateway to the server are encoded with the server public key, which is introduced in the gateway. Just the server can decrypt messages utilizing its relating private key. The private key is situated on the server and isn't shared with some other device. An asymmetric key cryptography approach is utilized between the gateway and the server because of the plenty of registeringcapabilities.

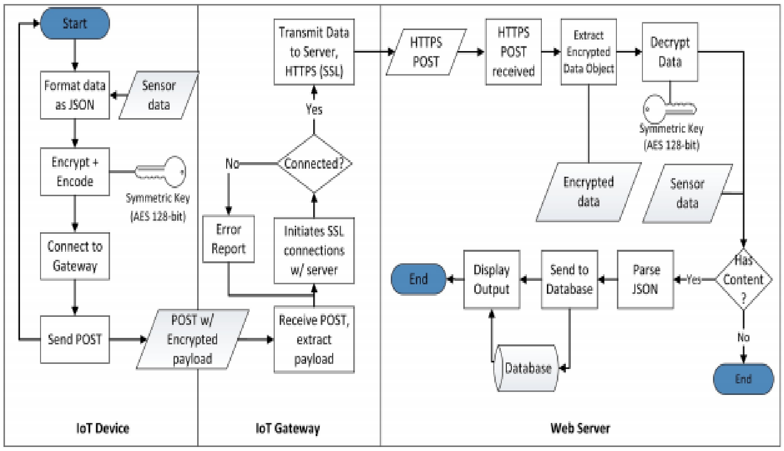

Figure 4: A full flowchart of the proposed security solution across the three IoT system components.

6. CONCLUSION

For the IoT security tending to issues, (for example, the Internet DNS assault), this theory proposes the IoT tending to security show. The customary get to control and the identity authentication just works in a similar layer. The IoT tending to security display designed in this postulation successfully understands the issues of vertically passing the authentication bring about the tending to process without changing the protocols for two communication parties. In addition, this postulation gives the question get to control and security assurance from the protest application layer tending to, DNS tending to and IP tending to stages.

7. REFERENCES

[1]. Lai, G. H. “Detection of wormhole attacks on IPv6 mobility-based wireless sensor network”. EURASIP Journal on Wireless Communications and Networking, Vol.1, 2016

[2]. Chen, C. M., Hsu, S. C., & Lai, G. H. “Defense Denial-of-Service Attacks on IPv6 Wireless Sensor Networks”, In Genetic and Evolutionary Computing, Springer International Publishing, pp. 319-326, 2016

[3]. Kharkongor, C., Chithralekha, T., & Varghese, R. “Trust and Energy-Efficient Routing for Internet of Things—Energy Evaluation Model”, In Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications, Springer, pp. 585-597, 2017.

[4]. Airehrour, D., Gutierrez, J., & Ray, S. K. “A Lightweight Trust Design for IoT Routing”. In Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd IEEE Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress, pp. 552-557, 2016

[5]. Jøsang, Audun, Ross Hayward, and Simon Pope. "Trust network analysis with subjective logic", Proceedings of the 29th Australasian Computer Science Conference, Vol.48, 2006.

[6]. Lize, G., Jingpei, W., & Bin, S. (2014). Trust management mechanism for Internet of Things. China Communications, 11(2), 148-156.

[7]. Peraković, D., Periša, AM., &Cvitić, I. (2015, January). Analysis of the IoT impact on volume of DDoS attacks. In 33rd Symposium on New Technologies in Postal and Telecommunication Traffic (PosTel 2015) (pp. 295-304).

[8]. Afreen, N. Fahmina , Basha, M. Mahaboob , Das, S. Mohan (2017) –“Design and implementation of area-delay-power efficient”, CSLA based 32-bit array multiplier

[9]. GauravVaswani,Anuradha Bhatia, 2013.” A Real Time Approach with BIG Data – A review”. Published by International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 9, ISSN: 2277 128X.