International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 6, Issue 10, pp 119-121, October-2022

https://doi.org/10.47001/IRJIET/2022.610021

IoT of Security Protocol

[1]Prof. S.B. Bele, [2]Dhanashri Dahake, [3]Pallavi Barange, [4]Sapna Bagde

[1]Assisant Professor, Department of MCA, Vidyabharati Mahavidyalaya, Amravati, India
[2,3,4]Student, Department of MCA, Vidyabharati Mahavidyalaya, Amravati, India

***Abstract* - The Internet of Things (IoT), is a network of devices that are uniquely identified and has embedded software required to communicate the transient states and data that are usually used to trigger an actuator. The edge networking devices and protocols are used to communicate with a cloud server that processes and aggregates the big data arriving from various devices, performs analytics and aids in business decisions. IoT has become an integral part of today's industrial, agriculture, healthcare and smart city revolution. Securing all entities involved in an IoT network is vital as it involves pervasive data collection and dissemination. Current IoT protocols work with IP protocols as backbone, but they are specially designed to operate in multiple layers and provide security at various layers. This chapter focuses on IoT protocols that deal with securing an IoT network. The major challenges in securing an IoT network is lack of standardization at manufacturing level which exposes the hardware, software and the data to various threats and attacks. The IoT protocols have to deal with security breaches at the site of the cloud service provider and the security issues pertaining to data privacy, authentication, authorization and trust management in a distributed heterogeneous environment. This chapter also elaborates on various security attacks and the solutions offered by IoT protocols.**

Keywords: IoT Security. IoT Architecture. IoT Protocols. IoT Threats IoT Attacks.

I. INTRODUCTION

In our research paper the Internet of things (IoT) environment is a collection of devices which are interconnected to each other. The devices in IoT are called as sensors/nodes. A node can be any of application specific sensors, mobiles, large computational devices etc. The IoT systems support the identification of these nodes or sensors within the desired ranges.

The devices attached to an IoT domain are remotely controlled or accessed. This concept is being defined in the IoT framework. As a result of these IoT specifications there have been significant advantages along the proficiency, precision, and financial considerations. The errors that could have occurred due to the manual interception is also reduced. Today we find the implementation of the IoT systems around several areas of the world. These developments suggest the significant increase of the IoT networks and the devices involved in this environment, for example, smart homes, wearable, smart city, smart grids, connected cars, industrial internet, connected healthcare, smart retail, smart supply chain, smart farming. Analyzed to see if any functional information that is of benefit to a customer or business could be retrieved. Essential elements of IoT are people, things, data and process. IoT systems aims at networking these elements that communicates with each other through wired or wireless medium.

II. IOT SECURITY REQUIREMENTS

Security must be addressed throughout the lifecycle of an IoT device. Shipley [1] and Jing et al. [2] lists security requirements to be checked at various stages of the life cycle in order to alleviate an IoT attack. IoT security requirements are listed below, Cryptographic Algorithms—Symmetric algorithms are light weight compared to asymmetric algorithms and hence were recommended for securing data transmission. However, they have problems in key exchange, confidentiality, digital signature and message authentication. Hence public key algorithms were recommended as they were able to provide key management, node authentication, scalability and security.

- Key Management Techniques - Key management is an important security feature in IoT. Light weight secure key distribution is required for secure communication.

III. IOT SECURITY ISSUES

The issues associated with security of IoT are not only the issues related with security of wireless medium, WSN and internet, but also access control, authentication and privacy issues associated with IoT.

- Low power embedded device - IoT devices have less computation power and storage capacity. It is often found embedded in a bigger hardware or wearable device where it is difficult to execute security algorithms that are normally heavy weight and expensive for a resource constrained device.
- Trust Management - Trust management is required for data authentication data gathering and dissipation phases

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 6, Issue 10, pp 119-121, October-2022
https://doi.org/10.47001/IRJIET/2022.610021

for which strong cryptographic techniques or digital signatures are recommended.

IV. IOT SECURITY CHALLENGES

Lists the challenges of IoT security based on limitations of hardware, software, network connections. The hardware limitations are computational and energy constraint, memory constraint and tamper resistant packaging. Limitations on software are embedded software constraint and dynamic security patch. Limitations on network connections are mobility, scalability, multiplicity of devices and communication medium, multi-protocol networking and network topology.

1. IoT Hardware
2. IoT Software and Firmware
3. Insecure Network Communication
4. Data Leaks from Cloud
5. Threats and Attack Vectors

V. IOT PROTOCOL ARCHITECTURE

IoT protocol stack is not standardized as TCP/IP or OSI protocol suite. Most of the IoT security protocols are designed to operate in multiple layers to provide security.

VI. IOT SECURITY ATTACKS

Internet of Things, the increasing need in our day-to-day life has more advantages. The important thing about IoT is, it makes the things beings intelligent by embedding sensors and actuators. By increasing the connectivity, it enables new services. On the other side, the amount of data generated by IoT is getting increased which results in security attacks.

Well, most of the people can think of

- Why Security is more important in IoT?
- What can a person do by attacking the device?
- Why is it important to consider the attack on device?
- Is it possible for my device to provide private data to intruders?

VII. IOT SECURITY SOLUTIONS

In the previous section, we briefly discussed about the possible attacks that can be performed on an IoT device. In this section, we will discuss about the protocol stack of IoT architecture, various protocols that supports the architecture and the various solutions to enhance the security of IoT devices. The protocol stack of IoT is shown in figure.

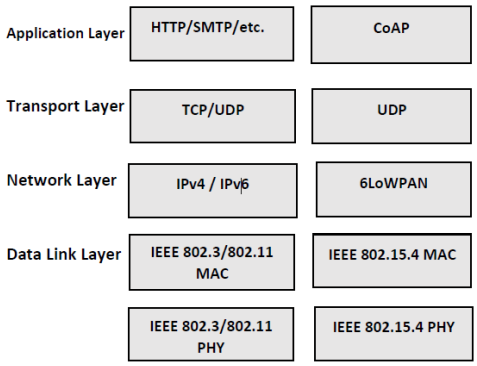

Figure 1: Protocol stack of IoT

Objective

Ten Security Objectives to Consider While Building An IoT Or IoT Product,

1. Security by Design
2. Privacy by design
3. Authentication and Authorization
4. Data Encryption and Access Control
5. Hardware Security 6] Network Security
6. Compliance Requirements
7. Performance Requirements
8. Regular Secured Updates
9. Event Logging Mechanism

Scope

1. MQTT
2. CoAP
3. DTLS
4. 6LoWPAN
5. ZigBee

Advantages

- It is capable of many to many broadcasts.
- Support publish- subscribe messaging queue.
- This protocol is light in weight and offers efficient data transmission.
- MQTT offer reduced network bandwidth in communication.

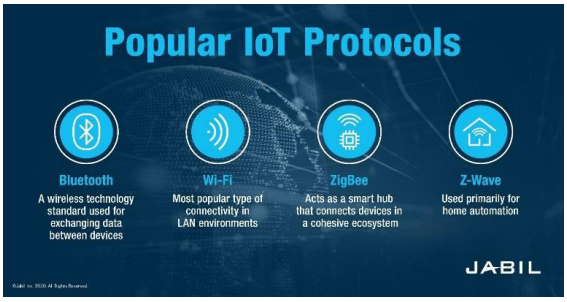

Figure 2: Popular IoT Protocols

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 6, Issue 10, pp 119-121, October-2022

https://doi.org/10.47001/IRJIET/2022.610021

Probable Output

IoT Security Solutions:

- Transport Layer Solutions
- Application Layer Solutions
- Network Layer Solutions

VIII. CONCLUSION

IoT system proposes several requirements in their design for implementing the security methods like CIA trends and few more. As required, IoT also impends a security architecture incorporated from ISO Protocol stack including layering architecture consisting of protocols at each layer. The protocols define their security proposals according of the requirement of their layers. The important protocols among the IoT can be CoAP, IEEE 802.15.4, RPL, Quic, CCIN, etc. Every protocol consists of their own header format and frame format. These includes own fields differing from one protocol to another. The security mechanism implemented also varies from one protocol to another. Thus all these works together in a layered fashion providing necessary security for the IoT environment.

REFERENCES

[1] Shipley AJ (2013) Security in the internet of things, lessons from the past for the connected future. Security Solutions, Wind River, White Paper 2. Jing Q, Vasilakos AV, Wan J, Lu J, Qiu D (2014) Security of the internet of things: perspectives and challenges. Wireless Netw 20(8):2481–2501.

[2] Vikas B O, Department of Computer Science and Engineering, SCE Bangalore, "Internet of Things (IoT): A Survey on Privacy Issues and Security".

[3] Surapon Kraijak, Panwit Tuwanut, King Mongkut's Institute of Technology Ladkrabang, "A survey on iot architectures, protocols, applications, security, privacy, real-world implementation and future trends".

[4] William M.S. Stout, Vincent E. Urias Sandia National Laboratories, "Challenges to Securing the Internet of Things".

[5] Arsalan Mohsen Nia, Student Member, IEEE and Niraj K. Jha, Fellow, IEEE, "A Comprehensive Study of Security of Internet-of-Things".

[6] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues".

[7] Teng Xu, James B. Wendt, and Miodrag Potkonjak Computer Science Department, University of California, Los Angeles, "Security of IoT Systems: Design Challenges and Opportunities".

[8] Minela Grabovica, Drazen Pezer, SRdan Popic, Vladimit Knezevic, "Provided security measures of enabling technologies in Internet of Things (IoT): A survey".

[9] Surapon Kraijak, Panwit Tuwanut, Information Technology Faculty, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand, "A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends".

[10] Prashanth Pomple Gurunath Chavan, "A Survey: Attacks on RPL and 6LoWPAN in IoT".

[11] Poulami Das, Debapriya Basu Roy, and Debdeep Mukhopadhyay, "Secure Public Key Hardware for IoT applications".

[12] S. Zamfir, T. Balan, I. Iliescu, F. Sandu, Department of Electronics and Computers, Transilvania"University, Brasov, Romania, "A Security Analysis on Standard IoT Protocols".

[13] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research issue".

Citation of this Article:

Prof. S.B. Bele, Dhanashri Dahake, Pallavi Barange, Sapna Bagde, "IoT of Security Protocol" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 6, Issue 10, pp 119-121, October 2022. Article DOI https://doi.org/10.47001/IRJIET/2022.610021

****

