Journal of Network and Information Security
9 (2) 2021, 14-18
http://www.publishingindia.com/jnis

Application Layer in Internet of Things: A Review in Protocols and Security Threats

Parvathy K.
Assistant Professor, Department of Computer Science and Engineering, Sri Ramakrishna Institute of Technology, Coimbatore, Tamil Nadu, India. Email: parvathy.cse@srit.org

Abstract: An Internet of things is an emerging technology are used in wide range of smart applications as smart cities, smart health, smart fitness, smart agriculture, smart home and other applications like institutions and military areas. They are aggregated together many interconnected devices which connects with an internet and various sensors. An IoT architecture is divided into various layers as perception layer, network layer and application layer. Due to wide usage of these smart devices, lack on security takes place and has the possibility of occurring the attacks. In this review paper, deep description on application layer protocols like Constrained Application Protocol (CoAP), Message Queuing Telemetry Transport (MQTT), Advance Message Queuing Protocol (AMQP) and REST (Representational State Transport) etc. and security threats on application layers and its attacks that care classified as web & mobile application and RFID attacks are represented.

Keywords: Application layer, Architecture layers, Internet of Things, Security threats.

I. Introduction

The Internet of Things [1] is discovered by Kevin Aston in the year 1999, by a group of interconnected devices that can be in wired or wireless form and share the data. In Internet of Things the main concerns are reliable network and secure data transmission. It needs a network by need of sensors and the devices by sharing, processing and enabling them. The IoT [3] is said to be a complex environment, where the smart devices are connected in between them by the heterogenous form. The communication is performed by a shared infrastructure and good protocol standard. The privacy protection is the main challenges in IoT. [4] in IoT are used in many applications with smart devices like agriculture, health, fitness, roads, Institutions and military areas etc. IoT can be of low in cost, high performance of hardware, high speed of machine to machine (M2M).

Application layer [3,11] of IoT is defined where the layer that works on mobile and web-based applications. This layer is said to be a topmost layer in the architecture of IoT. The layer is above of the transport layer by the layer like TCP/IP protocol stack comes in both the transport and application layer of IoT and access network services world wide web (WWW) uses the application layer protocol called hypertext transfer protocol (HTTP). To optimize the HTTP, REST architecture is used. In [5] an application layer two protocols are specifically designed they are as MQTT and CoAP. MQTT is manufactured by IBM, an optimized application layer protocol for messaging and is used for pub/sub-based system. CoAP, by Internet Engineering Task Force. It is designed for constrained devices with low processing and memory devices. In this paper, a brief review on IoT Architecture layers and a review on application layer of IoT as protocols and its types are represented and attacks in application layer in IoT are well explained.

II. Related Work

An introduction [1] on internet of things applications of IoT Illustrates well. [3, 4, 11] discusses about the IoT architecture and its schematic diagram. It represents various layers in IoT architecture as perception layer, network layer and application layer. [5, 6, 7, 10, 11] the application layer is discussed the protocols and its types they are as MQTT, AMQP, CoAP, XMPP, DSS and REST. [8] discuss about MQTT they are is known as Message Queue Telemetry Transport. The application layer protocol is most widely light weight protocol. [9] which illustrates the protocol called AMQP, they are called as Advance Message Queuing Protocol; it is a middleware messaging and open standard application layer protocol. [10, 11] discuss about CoAP. They are known as Constrained Application Protocol, this protocol is made for the subset of HTTP methods. The protocol [11] called XMPP is called as Extensible messaging and presence protocol. This is an application layer protocol which uses for real time communication. DDS [12] is known as Data Distribution Service. It is datacentric protocol. It uses both machine-to-machine and device-to-device communication. REST [13] stands for Representational State Transfer which uses as HTTP application layer protocol.

III. Internet of Things Architecture

In IoT, [4, 10] there is a lack of consistency and standards across all over the world due to the reasons of interoperability,

compatibility and manageability. An IoT are constructed in variety of devices based on topologies of the network they are as star, clustered trees, tree and mesh. In an IoT, [3, 5, 6] the "Things" which comprises various communication protocols such as LoRaWAN, 802.15.4, Bluetooth Low Energy (BLE) and Zigbee. The IoT platforms serve in large high-tech companies like Amazon AWT IoT, Microsoft azure suite, Samsung Artik cloud, and Google Cloud etc. The IoT Architecture is subdivided into various layers they are as follows: 1) Perception layer 2) Network layer and 3) Application layer.

A. Perception Layer

The [3] first layer of architecture which has PHY layer and MAC layer. The PHY layer is used in the hardware like sensors and devices. The MAC layer creates a connection between a device and the network to find a proper communication. The protocols used in MAC layer are as follows: Cellular network (LTE M, EC-GSM), PAN (IEEE 802.15.4e, Z-Wave), LAN (IEEE 802.11ah).

B. Network Layer

The network protocols [5, 6] works as transmission for information and data storage. The transmission needs of certain protocols like GSM, WiFi, 3-5G, LTA, IEEE 802.15.4 IPv6 etc. These protocols connect with smart devices for the transmission. For secure transmission data encryption technique is used and thus authentication is clearly performed by the clear verification of the process.

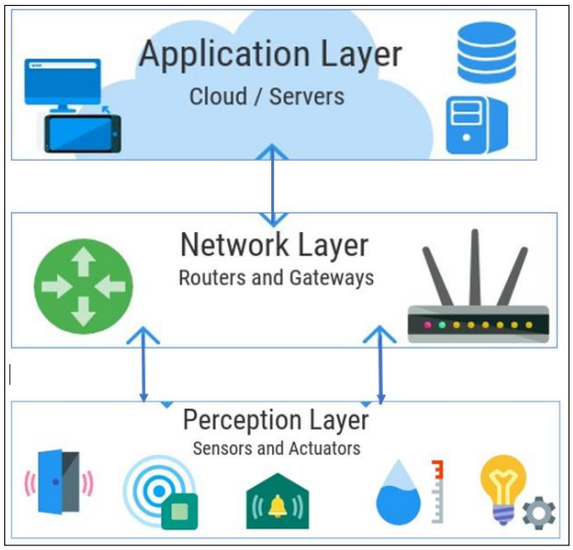

Fig. 1: IoT Architectural Layers

C. Application Layer

The third layer [7, 8] of the architecture mainly works in mobile and web-based softwares. In IoT numerous amounts of applications were used i.e., Living space/homes/building, transportation, health, education, agriculture, business/trades, energy distribution system, etc. Protocols used in this layer are as follows: LTP, HTTP, CoAP, DNP, DDS, AMQP, SSH and IPfix etc.

IV. Application Layer in Internet of Things (IOT)

In IoT architecture, [10] this layer situates in the third part which works in more on mobile and web-based softwares. This part which illustrates more on application layer protocols and attacks.

A. Application Layer Protocols

Depending upon the network usage and the suitability of the application layer various protocols are introduced they are as follows: MQTT, AMQP, CoAP, XMPP, DSS and REST. Fig. 2 shows various application layer protocols.

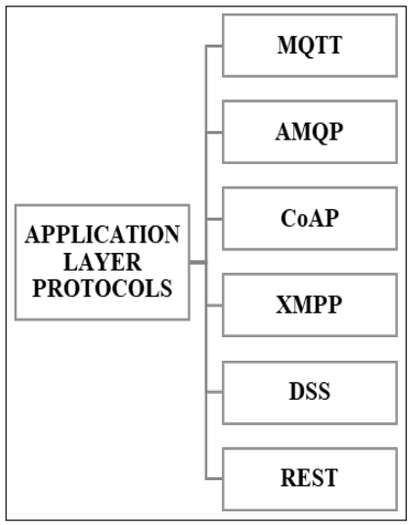

Fig. 2: Application Layer Protocols

MQTT [8] is known as Message Queue Telemetry Transport. The application layer protocol is most widely light weight protocol on publish-subscribe model. This protocol is used for analyzing the connected smart devices and mobile devices to application in a centralized data collection. [9] This case is said to be optimized. There are three types of Quality of services they are QoS0, QoS1 and QoS2. Qos0 is called At most once where it sends message only one time. The publisher sends data to broker and in the response doesn't wait for acknowledgement. QoS1 is called as At least once. This category may increase of reliability and overhead. The publisher waits for ACK (APUBACK) from broker. If the ACK is not received after the time interval, data is retransmitted. QoS2 is called as Exactly once. Publisher sends data to broker and wait for Publish Receive (PUBREC) the PUBREC is received, it discards the reference to published data and Publish Released (PUBREL) to the broker.

AMQP [9] is called as Advance Message Queuing Protocol, it is a middleware messaging and open standard application layer protocol. The features include message orientation, queuing, switching, reliability and security. These protocols reinforce both point-to-point and publisher/subscriber models.

CoAP [10, 11] is known as Constrained Application Protocol, this protocol is made for the subset of HTTP methods. Since it is a lightweight it uses UDP protocol. It regulates on request-response model for the communication between client and server. CoAP need the requirement for M2M communication. CoAP consist of two Quality of Service Mechanism they are Confirmable Message and Non-confirmable Message. The Confirmable message needs reliability by implementing retransmission mechanism. These types uses the acknowledgment method. Non-confirmable Message is a send and forget method where there is no need of acknowledgment method.

XMPP [11] is called as Extensible messaging and presence protocol. This is an application layer protocol which uses for real time communication and XML data between the network entries. For client server architecture these protocols are used in a decentralized form. It reinforces server-server and client-server communication protocols.

DDS [12] is known as Data Distribution Service. It is datacentric protocol. It uses both machine-to-machine and device-to-device communication. It contributes on reliability and good Quality of services. It is a middleware standard protocol and it is the first international standard protocol. This protocol which addresses on embedded and real-time system.

REST [13] stands for Representational State Transfer which uses as HTTP application layer protocol. REST uses methods by HTTP they are as follows: GET, PUT, POST, DELETE etc. GET and PUT are used to retrieve and send the data. PUT used to update the data. REST uses simple request/response model. Table I shows the application protocol features.

Table I: Features of Application Layer Protocol

Application Layer Protocol	Model	QoS	Secured State
MQTT	Publish-subscribe model	Yes (3 types)	Yes
AMQP	Point-to-point and publish subscribe model	Yes	Yes
CoAP	Request-response model	Yes (2 types)	Yes
XMPP	Server-server and client-server Protocols	Not sure	Yes
DDS	M2M and device communication Protocol	Yes	No
REST	Request-response model	Yes	Yes

B. Security Threats in Application Layer

In [14, 15] Internet of Things, interconnection of devices and network group together and perform the data communication. Due to the wide range of usage the data may be in insecure state and attacks may occur. In this scenario security goals are very important they are CIA triad as Confidentiality, Integrity and Availability.

1) Confidentiality

The term [14] is defined as by creating a secure connection so that the data can be accessed to the authorized users. It is an encryption mechanism. These techniques are used in mainly biometric analysis of a user.

2) Integrity

The data integrity [15] is an integrated network, where the data can be secured from the attackers by using communication mechanism. The detection methods for data integrity are Checksum and Cyclic redundancy check (CRC).

3) Availability

The IoT Security [15] that provides a data during the communication. The data is available to the authorized user. For the prevention from the attacks the countermeasure is firewalls. It prevents the denial-of-service-attacks by preventing the availability of the data to the unauthorized user.

C. Security Attacks in Application Layer

Nowadays, [12] smart technology is growing fast with various devices and sensor which uses in various applications. The application that can be smart fitness, smart grid, smart agriculture, smart city etc. Due to the wide usage of smart devices, it has the possibility to occur attacks and damage the whole IoT networks. The security attacks in application layer are classified as in two ways one is web and mobile application and RFID. Table II shows the security attacks in Application layer.

1) Web and Mobile Application Attacks

The IoT applications [13] are functioning with a wide usage of mobile and web applications. The intruder comes to these

applications and cause attacks. There are different types of attacks in web and mobile application they are as DoS, Repudiation, Malicious code, data corruption and eavesdropping.

The [6] intruder as an inactive state act as an authenticated user and access to the system and get into the network and cause to vulnerability to the system.

The [7] attacker injects malicious code to the system from unknown location and snatch or manipulate the data of the authorized user.

A repudiation attack [7, 8] is allowing malicious manipulation or forging the identification of new tasks or the data, where an application or system does not properly track and log users' task by considering invalid or misleading to the data storage.

The [9] data corruption is also called as a ransomware attack where the data like files are been in corrupted state as files and database corruption. The file which cannot able to perform the encryption properly is called as data corruption. The data that cause attacks i.e., been corrupted state through SQL queries is called as database corruption.

An eavesdropping attack, [10] also known as a sniffing or snooping attack. The attack is occurred when the data is transmitted during the communication in any IoT smart devices, by stealing the information during the process. The attack which accesses data which is in unsecured state during the communication or data transmission.

TABLE II: TYPES OF ATTACKS IN APPLICATION LAYER

Web and Mobile Application Layer Attacks	RFID Attacks
DoS	Unauthorized Tag Reading
Repudiation	Tag Modification Attack
Malicious Code	Software Attack
Eavesdropping	
Data Corruption	

2) RFID Attacks

Attacks [4] which focus on application layer cannot cause to only the application, it also causes the whole IoT devices. attacks happen to be when the application gives the comparison of joined RFID tags and clients in an IoT devices. The attacks in RFID application layer are unauthorized tags reading, tag modification, and the middleware attacks.

Software attacks [4, 5, 6] which are based on Software based vulnerabilities and communication interface loopholes which are the major rootcause to the software-based attacks. The types of attacks are occurred when a basically based on the hypothesis that human make an error by transmitting the information in IoT devices that cause the problem in it. Some of the threats in these attacks are Trojan horse programs, buffer overflows, viruses, boot loader worms, and injection of infected code.

Unauthorized tag [7] reading is defined during the read operation the protocol known as authentication protocol which is not have the supportability, in this reason it is tough for the intruder to get into it. Many number of RFID things are connected with IoT for the securing of authentication and authorization. The RFID things is having a tag called RFID tags that helps the information to be protected from the attacker and also cannot able to rechange or modify and delete the data in an information.

Tag modification [7, 8, 9] is when a wide usage of RFID tags that can have the possibility of modifying the data and easy access of data to the attacker. The intruder who get into the data and change or modify them with a malicious code to make it as attack effected data.

V. CONCLUSION

An IoT is a trending technology that are used in wide range of applications. An IoT Architecture is divided in various layers as perception layer, Network layer and Application layer. In this paper the representation on IoT and it's layer are briefly discussed. In IoT Architecture layer, the third layer called Application layer which is a mobile and web-based applications are mention above. Moreover, the Protocols of application layer are represented with an IoT and well description on Security threats in Application layer by classifying the attacks in RFID and application layer attacks. In future, this review can be applicable to other layers in IoT architecture as well.

REFERENCES

[1] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *Journal of Network and Computer Applications*, vol. 161, Jul. 2020, Art. no. 102630.

[2] K. Aarikaa, M. Bouhlal, R. A. Abdelouahid, S. Elfilali, and E. Benlahmar, "Perception layer security in the Internet of Things," *Procedia Computer Science*, vol. 175, pp. 591-596, 2020.

[3] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and Muhd. Imran, "Perception layer security in Internet of Things," *Future Generation Computer Systems*, 2019.

[4] S. Sharma, and H. Sain, "Fog assisted task allocation and secure deduplication using 2FBO and MoWo in cluster-based industrial IoT (IIoT)," *Journal of Computer Communications*, vol. 152, pp. 187-199, 2020.

[5] M. S. S. Rukmini, and Y. U. Devi, " IoT in connected vehicles: Challenges and issues - A review," in *Proceedings of the IEEE International Conference*

on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, 2016, pp. 1864-1867.

[6] U. Tandale, B. Momin, and D. P. Seetharam, "An empirical study of application layer protocols for IoT," *International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017)*, 2017.

[7] J. Ma, H. Yu, Y. Xu, and K. Deng, "CDAM: Conservative data analytical model for dynamic climate information evaluation using intelligent IoT environment - An application perspective," *Journal of Computer Communications*, vol. 150, pp. 177-184, 2020.

[8] S. Arvind, and V. A. Narayanan, "An overview of security in CoAP: Attack and analysis," *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, 2019.

[9] R. A. Rahman, and B. Shah, "Security analysis of IoT protocols: A focus in CoAP," *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, 2016, pp. 1-7.

[10] K. P. Naik, and U. R. Joshi, "Performance analysis of constrained application protocol using Cooja simulator in Contiki OS," *2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, 2017, pp. 547-550.

[11] P. Sharma, M. Kherajani, D. Jain, and D. Patel, "A study of routing protocols, security issues and attacks in network layer of Internet of Things framework," *2nd International Conference on Data, Engineering and Applications (IDEA),* 2020.

[12] H. P. Alahari, and S. B. Yalavarthi, "A survey on network routing protocols in Internet of Things (IOT)," *International Journal of Computer Applications*, vol. 160, no. 2, Feb. 2017.

[13] Internet Users. Accessed: Dec. 14, 2017. [Online]. Available: http://www.Internetlivestats.com/Internet-users/

[14] Global Internet Usage. Accessed: Dec. 14, 2017. [Online]. Available: https://www.en.wikipedia.org/wiki/Global_Internet_usage/

[15] Muhd. Burhan, R. A. Rehman, B. Khan, and B.-S. Kim, "IoT elements, layered architectures and security issues: A comprehensive survey," *Sensors,* vol. 18, no. 9, 2018, Art. no. 2796, doi: 10.3390/s18092796,www.mdpi.com/journal/sensors.