Security Threats in the Application layer in IOT Applications

Sowmya Nagasimha Swamy
Dept. of Information Technology,
Ramrao Adik Institute of Technology,
Nerul, Navi Mumbai, India
sownag@gmail.com

Prof. Dipti Jadhav
Dept. of Information Technology,
Ramrao Adik Institute of Technology,
Nerul, Navi Mumbai, India
Jadhav_dips@yahoo.co.in

Prof. Nikita Kulkarni
Dept. of Information Technology,
Ramrao Adik Institute of Technology,
Nerul, Navi Mumbai, India
nikitajkulkarni@gmail.com

***Abstract*— The Internet of things aspires to connect anyone with anything at any point of time at any place. Internet of Thing is generally made up of three-layer architecture. Namely Perception, Network and Application layers. A lot of security principles should be enabled at each layer for proper and efficient working of these applications. This paper represents the overview of Security principles, Security Threats and Security challenges at the application layer and its countermeasures to overcome those challenges. The Application layer plays an important role in all of the Internet of Thing applications. The most widely used application layer protocol is MQTT. The security threats for Application Layer Protocol MQTT is particularly selected and evaluated. Comparison is done between different Application layer protocols and security measures for those protocols. Due to the lack of common standards for IoT protocols, a lot of issues are considered while choosing the particular protocol.**

Keywords— component; Internet of Things; Application layer; Security threats; MQTT; Smart devices;

I. Introduction (Internet of things)

The Internet of Things was first Invented by Kevin Ashton in 1999. Internet of Things is the collection of many interconnected devices, objects, services, human which can communicate through wired/wireless mode and share data, information to achieve particular goal or applications. Internet of Things provides a Virtual connectivity through the Internet Protocol to Real life objects. Internet of Things provides the connectivity between objects timelessly.

Reliable Network and Secured Data Transmission and Privacy are the main Concern for any Internet of Things applications. As Internet of Things is a complex, Heterogenous interconnected system of Smart devices, communication of such devices is associated with the shared Infrastructure and common standard. Privacy Protection is the main challenge for any of the Internet of things application.

This paper main focus is on the Internet of Things Security threats at the Application layer. The Internet of Things architecture is assumed to be made up of three layer, namely perception, Network and application layers. This paper focus mainly on the Application layer protocols. As the application layer protocols plays an important role in all of the Internet of things application, security at this layer is very important and crucial. There are many application layer protocols for different Internet of things applications. Depending upon the application and rate of data transmission, time, heterogenous infrastructures and smart devices available, particular protocol is selected. The main aim of these protocol is to identify, track, monitor and manage the smart devices present in the network.

We can find many applications of Internet of things in almost all fields. Internet of things is an Intelligent network of different smart devices which can be identified, positioned, tracked, monitored and managed remotely.

Few applications of the Internet of things are as follows, Smart parking systems, Electro Magnetic level detection system, Structural Health monitoring system, Urban noise maps, Smart phone Detection, Traffic congestion, Smart lighting system. Waste Management system, Smart roads.

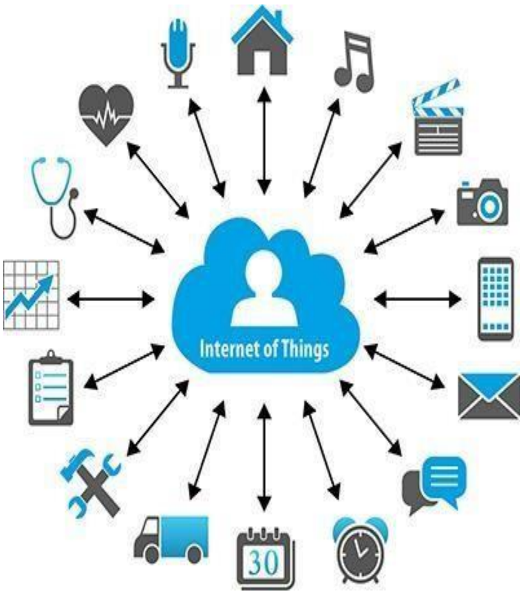

Fig: Internet of Things

II. Literature Survey

A. General Architecture

The Internet of things architecture is made up of three-layers. Namely Perception, Network and Application layers. In Internet of Things each layer is defined to perform particular task and functions. Each layer of Internet of Things has inherent security issues associated with it. The perception layer collects information from the real-time objects. This layer is also known as the "Sensors" layer of Internet of things. The main aim of this layer is to acquire or collect the information from the Environment using the Sensors and Actuators. It collects data and transmit it to the network layer for further processing. It also performs the internet of things Node collaboration in the local and short range networks.

Next layer is the Network layer, which acts like the Central Nervous system in the whole network. The main function of this layer is data Routing and transmission to different Internet of things hubs and devices over the Internet. The cloud computing platform, Routing, Switching and Internet Gateways and other devices acts in this region using the Bluetooth, ZigBee, Wi-Fi, LTE, 3G etc. Data aggregation, Data filtering, and transmission also takes place at this layer.

The last layer is the Application layer, the Data Integrity, Data confidentiality and Data authenticity is guaranteed by this layer. The application layer protocols define the application interface with the lower layer protocols to send the data over the network. Application layer protocols enable process-to-process connections using ports. HTTP, CoAP, web socket, MQTT, XMPP, DDS, AMQP are the few application layer protocols.

B. Application layer protocols in the Internet of things

There are many application layer protocols, depending upon the application suitable protocol is selected and used in the network.

MQTT (Message Queue Telemetry Transport) -This application layer protocol is most widely used. This is light weight protocol on publish-subscribe model. This protocol is optimized for centralized data collection and analysis-connecting smart devices and mobile devices to application running in a data center. This protocol is best suitable for the network of lower bandwidth, limited memory resources.

AMQP (Advance Message Queuing Protocol)- This is one of the open standard application layer protocol for middleware messaging protocol. The best features of this protocol is that it can do message orientation, queuing, switching, reliability and security. This protocol supports both point-to-point and publisher/subscriber models and routing and switching.

CoAP (Constrained Application Protocol)- This application layer protocol is intended to use in the constrained environment with constrained resources and constrained network. It is a web transfer protocol and uses a request-response model. This protocol is designed to co-operate and work along with HTTP.

XMPP (Extensible messaging and presence protocol)- This is an Application layer protocol intended to use for real time communication and for streaming XML data between network entities. This has a many application like messaging, data syndication, gaming, multi-party chatting and voice/video calling. This is a decentralized protocol using a client server architecture. It supports both client-server and server-server communication paths.

DDS (Data Distribution Service)- This application layer protocol is data centric protocol used for machine-machine and device-device communication. This protocol uses the publish-subscribe model. This protocol provides the configurable reliability and quality of service. This is the first open international middleware standard protocol which addresses the real-time communication for embedded systems.

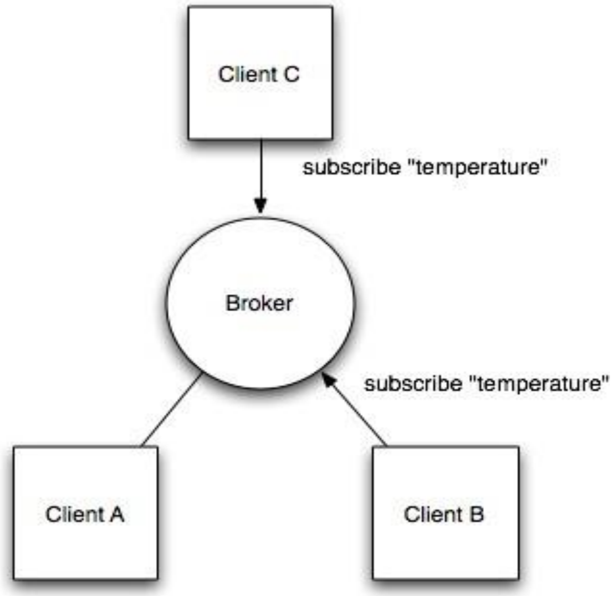

Fig.2 MQTT protocol

MQTT protocol:

The Application layer protocol are application depended. The choice of particular protocol depends upon many factors. The MQTT protocol is widely used protocol as this protocol can be used for the wireless and low-bandwidth networks. There are many projects that implements the MQTT protocol, example is Facebook messenger for online chatting, IECC Signaling Control system uses MQTT for communication within various parts of the system, Amazon Web services, Open Geospatial Consortium Sensor Things API uses MQTT, Open sources also uses the MQTT protocols.

The mobile application that uses MQTT protocol sends and receives messages by calling an MQTT library. The messages are transmitted through the MQTT messaging server. The MQTT client and server take in-charge of delivering messages for mobile app and manage the network management small. MQTT is also used for telemetry for receiving data from actuators and sensors and manage them remotely. To send and receive the messages, MQTT client library should be added to the application.

III. Security Threats and its measures

A. Security Goals

The important security goals of the Internet of things is to provide a reliable connection, and proper authentication mechanisms and provide confidentiality about the data to each device connected in the whole network. The information security triad, have suggested the CIA which is Data confidentiality, Integrity and Availability. Threats and breach in any of these areas could cause serious damage to the system and harm the reputation and have direct impact on the working of the system.

1) Data confidentiality

Data confidentiality refers to the ability to ensure privacy for the user by providing a secure connection to only the permitted users. The data can be accessed by the permitted user only. Data confidentiality can be achieved by data encryption mechanism where each bit of data is converted into cipher text and followed by two-step verification process, in which two devices/components allows access only if both the devices pass the authentication test, and a biometric verification in which the person is uniquely identifiable. In Internet of things, the devices ensure that sensor network nodes don't connect to neighboring nodes and tags don't transmit their data to unrecognized reader.

2) Data Integrity

Data Integrity is integrated in the network to secure data from cybercriminals during the communication mechanism, so that data tampering cannot be done without the system catching the threat. The Checksum and cyclic redundancy check are few error detection methods used to check the data integrity. Continuous syncing of data for backup purposes a version control is used.

3) Data Availability

The main goal of any Internet of things security is to provide the data to its users, whenever needed. The immediate access of data from the resources by its user not only in normal conditions but also in disastrous conditions should be possible. The firewalls are incorporated into the network to countermeasure the attacks on the services like Denial-of-service attack which can deny the availability of the data to the end user.

B. Application layer disputes

The few security disputes of the application layer are mentioned below:

1. Malicious code injection: In this technic, the unethical hacker injects malicious code from unknown location into the system and try to steal or manipulate the data of the authorized user.

2. Denial-of-service attack: In this attack the hacker pretend to be an authenticated user and log into the system and interrupt the normal working of the network. This is the biggest vulnerability to the system.

3. Phishing attack: This is an attack in which the email of the high-ranking authority in the network is used for attack. The attacker gains credentials access of that victim and damage data.

4. Sniffing attack: In this type, the attacker introduces a sniffer application into system to force an attack on it, which could gain network information leading to corrupted system and merges application and middleware layer to form an integrated security mechanism.

C. Security related Problems

1) Authentication of identity :

Different users will opt for different applications, each application will have huge number of users, so to prevent the illegal user getting into the system, proper authentication mechanism should be deployed.

2) Data storage and recovery:

The data storage involves the data transmission through different channels to different locations, which involves the user privacy, integrity of data. And later recovery of that data on time. Many security threats occur at the transmission of data. So, proper data storage and recovery should be incorporated at each and every step of data transmission.

3) Handling huge data:

There is large no of network nodes which are processing large amount of data, which leads to some of the data loss during the communication process which in turn affect the efficient working of the network.

4) Application layer software vulnerabilities:

Buffer overflow vulnerabilities may occur while programmer write non-standard codes in the software. Hackers may use this exploits to carry their purposes.

D. Security maesures

Few of the security measures to overcome the security problems are listed below,

1) Authentication: The authentication process restricts any malicious user from accessing the data, this process defends by integrated identity identifications. The cloud computing and virtualization are the main technology that are more prone to attacks. Insider threats for cloud computing and data theft, DOS attacks for the virtualization are most feared attacks. proper authentication technics should be employed.

2) Intrusion Detection: Intrusion detection technics produce the alarm on any suspicious activity in the system and provide an administer solutions for many threats by uninterrupted monitoring and cloud computing and virtualization technologies.

3) Risk Assessment: This method is used for identification of threats in the network and this process involves the situation analysis, comparison of various standards and checks for risks acceptance level.

4) Data security: The encryption methodologies is incorporated for data security. The same is achieved

by up-to-date anti-dos-firewalls and updated malwares and spywares.

IV. COMPARISION

TABLE I. COMPARISON TABLE OF DIFFERENT APPLICATION LAYER PROTOCOLS

Application layer protocols	**Protocol Features**				
	UDP/ TCP	***Architect-ure***	***Security and QoS***	***Header size (bytes)***	***Max-length***
MQTT	TCP	Pub/sub	Both	2	5
AMQP	TCP	Pub/sub	Both	8	-
CoAP	UDP	Req/res	Both	4	20
XMPP	TCP	Both	Security	-	-
DDS	TCP/ UDP	Pub/sub	QoS	-	-

Internet of things has many standard application layer protocols. These Application layer protocols are usually application dependent and these protocols are selected based on the requirements. Table 1 summarizes comparison points between these different application layer protocols. From above comparison table, we can conclude that MQTT, AMQP, CoAP protocols provide both Security and QoS. Future recommendations would be providing larger header size to these protocols. Universal standard should be applicable for all the protocols. The CoAP protocol is running on UDP, hence it is lightweight and recommended for few applications which requires the lower bandwidth.

V. CONCLUSION

The security parameters need to be focused further and the attention towards looking for new possible security solutions, so that Internet of things will be able to block all possible threats and vulnerabilities and provide secure services to the coming generation of data connected compliances. This paper briefly mentioned about the security goals, security threats and security challenges and probable solutions for securing the Internet of things system. In the future research and development process more authentications, severe risk assessment methods and intrusion detection techniques in each architectural layer must be incorporated in the security infrastructure. Also, a strong legal frameworks standard should be explored and regulations and policies must be made mandatory for all of the technologies.

VI. FUTURE WORK

Future work will be to implement the application layer protocols on different applications depending on the requirements and obtain the required data and compare among themselves. An Application server should be implemented to choose the appropriate protocol instantly without any application barrier, and without any common standard barrier. And particular protocol should be selected depending upon requirement, and network parameters availability.

REFERENCES

[1] M K Farooq Muhammad waseem "A Critical Analysis on the Security Concerns of Internet of Things (IoT)" by International Journal of Computer Applications (0975 8887) Volume 111 - No. 7, February 2015

[2] J.Satish Kumar, Dhiren patel "A Survey on Internet of Things: Security and Privacy Issues" by International Journal of Computer Applications (0975 – 8887) Volume 90 – No 11, March 2015.

[3] Eeshan Pandey*, 2Varshi Gupta "An analysis of Security Issues of Internet of Things "(IoT International Journal of Advanced Research in Computer Science and Software Engineering.

[4] Raghavendra K1, Sumith Nireshwalya "Application Layer Security Issues and Its Solutions "ISSN 2231-0711 vol 2 issue 6 1266-1269.

[5] Mayuri Bhabad,Sudhir T Bagade "Internet of Things: Architecture, Security Issues and Countermeasures" International Journal of Computer Applications (0975 – 8887) Volume 125 – No.14, September 2015.

[6] Reem Abdul Rahman and Babar Shah. "Security analysis of IoT protocols: A focus in CoAP". By MEC international conference.

[7] Qi Jing • Athanasios V. Vasilakos • Jiafu Wan • Jingwei Lu • Dechao Qiu "Security of the Internet of Things: perspectives and challenges "springer.

[8] Madhumita Panda ". Security Threats at Each Layer of Wireless Sensor Networks "International Journal of Advanced Research in Computer Science and Software Engineering.

[9] Tasos Kaukalias and Periklis Chatzimisios, Internet of Things (IoT) C Enabling technologies, applications and open issues, Encyclopedia of Information Science and Technology (3rd Ed.), IGI Global Press, 2014.

[10] Victoria Pimentel, Bradford G. Nickerson, Communicating and Displaying Real-Time Data with WebSocket, Internet Computing IEEE 16(4), July-Aug. 2012, pp. 45-53

[11] Shahid Raza, Hossein Shafagh, Kasun Hewage, Ren Hummen, Thiemo Voigt, Lithe:Lightweight Secure CoAP for the Internet of Things, Sensors Journal, IEEE 13(10), Oct. 2013, pp. 3711-3720.

[12] Dinesh Thangavel, Xiaoping Ma, Alvin Valera, Hwee-Xian Tan, Colin Keng-Yan Tan, Performance Evaluation of MQTT and CoAP via a Common Middleware, IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 21-24 April 2014, pp. 1-6.