International Advance Journal of Engineering, Science and Management (IAJESM)
ISSN -2393-8048, January-June 2020, Submitted in June 2020, iajesm2014@gmail.com

IOT Networks Security Perspective: A Review

Deepak Kumar Verma , Department of Computer Science and Engineering, University Institute of Engineering and Technology, Chhatrapati Shahu Ji Maharaj University, Kanpur-208024, India. deepak300572@gmail.com
Alok Kumar, Department of Computer Science and Engineering, University Institute of Engineering and Technology, Chhatrapati Shahu Ji Maharaj University, Kanpur-208024, India. akumar.uiet@gmail.com

Abstract

The widespread use of IoT in society has created a broad target for malicious actors to exploit. This concise paper introduces IoT and its security issues, covering its ecosystem and protocols. The paper then delves into the vulnerabilities present in IoT systems. Its intended audience is those with existing network knowledge but who are new to IoT. The study concludes that the shortage of IoT standards and limitations in device resources are critical issues. Opportunities exist for research into creating effective IoT Intrusion Detection Systems and energy-efficient cryptography techniques that can be reasonably deployed.

Keywords – IoT, MQTT, CoAP, AMQP, LoRaWAN, 6LoWPAN,

I. INTRODUCTION

The term "Internet of Things" (IoT) describes a collection of physical devices, such as home appliances, vehicles, and other objects, that are equipped with sensors, software, and connectivity to enable them to gather and share data with other devices and systems via the internet. [1]. IoT networks are the infrastructure that enables these devices to communicate and exchange data. The IoT infrastructure is a set of technologies and components that work together to enable the communication, management, and integration of IoT devices and systems. The infrastructure is made up of various layers, each responsible for specific tasks and functions.

The main layers of IoT infrastructure are:

IOT infrastructure includes following layers [2], [3], [4]

Devices: This layer includes the physical devices such as sensors, actuators, controllers, and other hardware that gather and process data from the environment.

Connectivity: This layer includes the network protocols, gateways, and communication technologies that enable devices to connect and exchange data with other devices and systems.

Cloud Platform: This layer includes the cloud-based services and applications that manage and process the data collected from IoT devices. It includes data storage, processing, and analytics, as well as security and management services.

Applications: This layer includes the software applications that use the data generated by IoT devices to provide value-added services and solutions to end-users. Examples include smart home automation, energy management, and predictive maintenance.

End-users: This layer includes the people or organizations that use and benefit from the IoT solutions and applications.

The IoT infrastructure plays a critical role in enabling the growth and development of the IoT ecosystem. It enables the integration of diverse devices and systems, improves data management, and enhances the scalability and flexibility of IoT solutions.

Security aspects in IOT networks

Security is a critical aspect of IoT networks because of the sheer number of devices and the sensitive data they collect and transmit. Here are some of the key security aspects that need to be considered in IoT networks:

1. Authentication and Authorization: IoT devices need to be authenticated and authorized before they can access network resources or transmit data. This is typically done using digital certificates, passwords, or biometric authentication.

2. Encryption: Data transmitted by IoT devices needs to be encrypted to prevent unauthorized access and ensure data confidentiality. Strong encryption algorithms such as AES or RSA should be used to secure data in transit.

3. Access Control: Access control mechanisms should be implemented to control who can access IoT devices, network resources, and sensitive data. Access control policies should be based on roles and permissions, and should be reviewed and updated regularly.
4. Secure Communication: IoT devices should use secure communication protocols such as HTTPS, MQTT, or CoAP to transmit data over the network. These protocols provide end-to-end encryption and can help prevent data interception and tampering.
5. Firmware Updates: IoT devices should be regularly updated with the latest firmware and security patches to protect against new threats and vulnerabilities. Firmware updates should be done securely to prevent unauthorized access or modifications.
6. Physical Security: IoT devices should be physically secured to prevent tampering or theft. Devices should be located in secure areas, and physical access to the devices should be restricted.
7. Security Monitoring and Incident Response: IoT networks should be continuously monitored for suspicious activity or security breaches. An incident response plan should be in place to detect, contain, and respond to security incidents in a timely manner.

IOT devices include

Actuators: Actuators are a type of transducer that carry out physical actions based on instructions received from their control centers, typically in response to changes detected by sensors.
Embedded systems: Embedded systems consist of both hardware and software components, and are designed to manage a specific function within a larger system. They are typically based on microprocessors or microcontrollers.
Intelligent devices: are capable of performing computations, and may be equipped with a microcontroller. They can also leverage services like Azure IoT Edge to efficiently deploy specific workloads across multiple devices.
Microcontroller unit: MPUs, or microprocessor units, perform the same functions as CPUs but on a single or multiple integrated circuits. While microprocessors need peripherals to accomplish tasks, they can significantly reduce processing costs by containing only a CPU.
Non-computing devices: These are devices that can only connect and transmit data, without any ability to perform computations.
Transducers: Transducers, in general, are devices that transform one form of energy to another. In the context of IoT devices, this includes the internal sensors and actuators that collect and transmit data as the devices interact with their surroundings.
Sensors: Sensors identify variations in their surroundings and generate electrical signals to transmit this information. These transducers are frequently used to detect environmental changes, such as fluctuations in temperature, chemicals, or physical orientation.

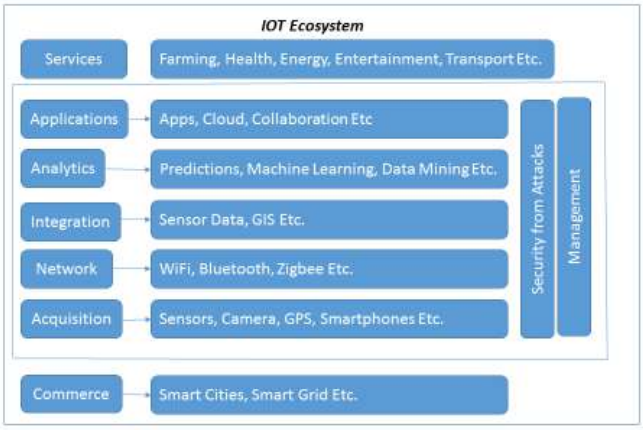

FIGURE-1 IOT ECOSYSTEM

IoT networks require a comprehensive security strategy that includes strong authentication, encryption, access control, secure communication, regular firmware updates, physical security, and security monitoring and incident response. By addressing these security aspects,

organizations can reduce the risk of IoT security breaches and protect their valuable assets and sensitive information.

Apart from other factors such as resource and power constraints, ensuring secure communication is crucial for IoT network security.

A. Confidentiality

The goal is to ensure that information sent to a node is not intercepted by unauthorized users or nodes, regardless of the number of nodes the message traverses, from the source to the destination.

B. Authentication

It is the process of accurately identifying a user or node to prevent impersonation.

C. Integrity

Refers to taking measures to safeguard messages from any unauthorized modifications or destruction as they travel from the source to the destination.

D. Non-repudiation

Non-repudiation ensures that an entity cannot deny having sent a message once it has been sent.

E. Availability

Ensures that the resources or services provided by the system on the network are accessible to authorized users.

II LITERATURE SURVEY

Protocols used for IOT network communication

There are several communication protocols used for IoT devices, each with its own advantages and limitations. some of the most commonly used protocols[5], [6], [7]:

1. MQTT: Message Queuing Telemetry Transport is a lightweight messaging protocol designed specifically for IoT devices. It is widely used in IoT applications, particularly those that require reliable communication with low network bandwidth and power consumption [8].

MQTT uses a publish /subscribe messaging model, where IoT devices can subscribe to specific topics and receive messages that are published on those topics. It is designed to be efficient and scalable, allowing IoT devices to communicate with each other and with the cloud without consuming excessive network resources.

One of the key advantages of MQTT is its support for Quality of Service (QoS) levels, which enable IoT devices to choose the level of reliability they require for each message. This allows devices to prioritize certain messages, ensuring that critical data is reliably delivered while minimizing network overhead for less critical data.

MQTT also provides security features, such as authentication, encryption, and access control, to ensure the confidentiality, integrity, and availability of data transmitted over the network.

2. CoAP: CoAP (Constrained Application Protocol) is a lightweight communication protocol designed specifically for IoT devices that have limited processing power, memory, and bandwidth. It enables IoT devices to communicate efficiently over constrained networks, such as low-power wireless networks.

CoAP is based on the Representational State Transfer (REST) architecture, and uses a client-server model, where IoT devices send requests to servers and receive responses. It is designed to be simple and efficient, with a small code footprint that can be easily implemented on resource-constrained devices.

One of the key advantages of CoAP is its support for caching and proxying, which enable IoT devices to save power and reduce network traffic by reusing previously requested data. CoAP also supports multicast communication, enabling multiple IoT devices to receive the same data with a single request.

CoAP provides security features, such as Datagram Transport Layer Security (DTLS), to ensure the confidentiality, integrity, and availability of data transmitted over the network. It also

supports Lightweight Machine-to-Machine (LwM2M) protocol, which enables IoT devices to be managed and controlled remotely.

It is a promising protocol for IoT communication, particularly in environments where low-power, low-bandwidth wireless networks are used. Its support for caching, multicast communication, and security features make it an ideal choice for IoT applications such as smart homes, smart cities, and industrial automation.

3. AMQP: Advanced Message Queuing Protocol AMQP (Advanced Message Queuing Protocol) is a robust and reliable messaging protocol that is designed for use in distributed and decentralized IoT systems. It enables different IoT devices and systems to communicate with each other, even when they are located in different networks or are running on different platforms [9].

AMQP is a binary protocol that provides a range of advanced messaging features, such as message queuing, routing, and reliability. It also provides support for a wide range of messaging patterns, such as request/response, publish/subscribe, and point-to-point messaging.

One of the key advantages of AMQP is its support for a variety of transport protocols, such as TCP, WebSocket, and TLS. This makes it possible for IoT devices to communicate with each other over different types of networks, including local area networks, wide area networks, and the Internet.

AMQP also provides security features, such as authentication, authorization, and encryption, to ensure the confidentiality, integrity, and availability of data transmitted over the network. It also supports Quality of Service (QoS) levels, which enable IoT devices to choose the level of reliability they require for each message.

4. Zigbee: It is a low-power, low-cost wireless communication protocol that is designed specifically for IoT devices. It is based on the IEEE 802.15.4 standard and operates in the 2.4 GHz frequency band. Zigbee is intended for use in small-scale, low-power wireless networks that require secure and reliable communication.

Zigbee uses a mesh networking architecture, where IoT devices can communicate directly with each other or through intermediary devices, such as routers or coordinators. This enables IoT devices to communicate over longer distances than they would be able to if they were communicating directly with each other.

Zigbee provides support for a variety of messaging patterns, including unicast, multicast, and broadcast messaging. It also provides security features, such as encryption, authentication, and authorization, to ensure the confidentiality, integrity, and availability of data transmitted over the network.

One of the key advantages of Zigbee is its low power consumption, which makes it ideal for IoT applications that require long battery life, such as smart homes and industrial automation. Zigbee also supports a range of data rates, from 20 to 250 kbps, which enables it to be used in applications that require different levels of bandwidth.

5. Bluetooth: Bluetooth is a wireless communication protocol that is widely used in IoT applications, such as smart homes, wearables, and healthcare. It is based on the IEEE 802.15.1 standard and operates in the 2.4 GHz frequency band.

Bluetooth is designed for short-range communication between IoT devices, typically within a range of about 10 meters. It supports a range of different messaging patterns, including point-to-point and point-to-multipoint communication.

One of the key advantages of Bluetooth is its low power consumption, which makes it ideal for IoT applications that require long battery life. Bluetooth also provides support for data rates up to 24 Mbps, which enables it to be used in applications that require high-speed data transfer.

Bluetooth provides security features, such as encryption and authentication, to ensure the confidentiality, integrity, and availability of data transmitted over the network. It also provides

support for Quality of Service (QoS) levels, which enable IoT devices to choose the level of reliability they require for each message.

6. LoRaWAN: Long Range Wide Area Network is a wireless communication protocol that is designed specifically for IoT applications that require long-range, low-power wireless networking. It operates in the sub-GHz frequency bands, such as 868 MHz in Europe and 915 MHz in the US [10], [12].

LoRaWAN uses a star-of-stars network topology, where end-devices communicate directly with gateway devices that are connected to a central network server. The network server then processes and routes the data to the appropriate application server. This enables IoT devices to communicate over long distances, up to several kilometers in rural areas and hundreds of meters in urban areas.

One of the key advantages of LoRaWAN is its low power consumption, which enables IoT devices to operate on a single battery for years. It also provides support for different data rates, from 0.3 kbps to 50 kbps, which enables it to be used in applications that require different levels of bandwidth.

LoRaWAN provides security features, such as encryption and authentication, to ensure the confidentiality, integrity, and availability of data transmitted over the network. It also provides support for Quality of Service (QoS) levels, which enable IoT devices to choose the level of reliability they require for each message.

7. Wave: This protocol, also known as the Web Application Verification Environment, is an open-source communication protocol designed specifically for IoT devices. The protocol uses a publish/subscribe messaging model and is based on the Extensible Messaging and Presence Protocol (XMPP).

One of the key features of the Wave protocol is its ability to handle intermittent connectivity, which is common in IoT networks. It uses a store-and-forward mechanism to ensure that messages are reliably delivered even when devices are temporarily offline.

The Wave protocol also supports end-to-end encryption and authentication, which helps to secure communication between IoT devices. It also provides flexible authorization policies that can be customized to suit the needs of different IoT applications.

Overall, the Wave protocol is a promising solution for IoT communication, particularly in environments with intermittent connectivity and strict security requirements.

Each protocol has its own advantages and disadvantages, and the choice of protocol depends on the specific requirements of the IoT application, such as power consumption, data rate, range, and reliability.

8. 6LoWPAN: IPv6 over Low-power Wireless Personal Area Networks is a communication protocol designed specifically for IoT devices that use low-power, low-bandwidth wireless networks. The protocol enables IPv6 communication over constrained wireless networks, such as IEEE 802.15.4-based networks commonly used in IoT applications [11].

6LoWPAN is designed to provide a lightweight and efficient communication protocol that can run on resource-constrained devices, such as sensors and actuators. It uses compression and header compression techniques to minimize the size of IPv6 packets and reduce the overhead of transmission. This enables IoT devices to communicate efficiently over low-power, low-bandwidth wireless networks, while also minimizing power consumption.

In addition to supporting IPv6 communication, 6LoWPAN also includes security features, such as link-layer encryption and authentication, to help secure communication between IoT devices.

6LoWPAN is a promising protocol for IoT communication, particularly in environments where low-power, low-bandwidth wireless networks are used. Its efficient use of network resources and security features make it a popular choice for IoT applications such as home automation, smart metering, and industrial control systems.

9.. Sigfox is a proprietary communication protocol designed specifically for IoT devices that require low power, long-range communication capabilities. It operates on the unlicensed Industrial, Scientific, and Medical (ISM) frequency bands and provides connectivity for devices that send small amounts of data over long distances [12].
The Sigfox protocol is designed to be simple, efficient, and easy to integrate with existing IoT devices. It uses a star network topology, where IoT devices transmit data to a central base station, which then forwards the data to the cloud for processing and storage.
One of the key advantages of the Sigfox protocol is its low power consumption. IoT devices using Sigfox can operate for years on a single battery charge, making it an ideal solution for remote monitoring and tracking applications.
The protocol also provides security features, such as encryption and authentication, to ensure the confidentiality and integrity of data transmitted over the network. Additionally, Sigfox has built-in geolocation capabilities, which enable IoT devices to determine their location without the need for GPS or other location-based technologies.
Overall, the Sigfox protocol is a popular choice for IoT applications that require long-range, low-power connectivity, such as smart agriculture, asset tracking, and remote monitoring.
TABLE-1 COMPARISON CHART WITH VARIOUS PARAMETERS FOR POPULAR IOT PROTOCOLS: MQTT, COAP, AMQP, ZIGBEE, BLUETOOTH, LORAWAN, WAVE, 6LOWPAN, AND SIGFOX.

Protocol	MQTT	CoAP	AMQP	Zigbee	Bluetooth	LoRaWAN	Wave	6LoWPAN	Sigfox
Data Transfer Method	Publish/ Subscribe	Request/ Response	Message Queues	Peer-to-Peer	Peer-to-Peer	Star Topology	Ad-hoc Mesh	Ad-hoc Mesh	Ultra Narrow Band
Network Topology	Broker-based	Client-Server	Point-to-Point	Mesh	Piconet	Star	Peer-to-Peer	Peer-to-Peer	Star
Communication Type	Asynchronous	Both	Synchronous	Asynchronous	Both	Asynchronous	Asynchronous	Both	Asynchronous
Quality of Service (QoS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bandwidth	Low	Low	High	Low	Low	Low	High	Low	Very low
Range	Short	Short	Long	Medium	Short	Long	Short	Short	Long
Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Power Consumption	Low	Low	High	Low	Low	Very low	High	Low	Very low
Standardization	OASIS Standard	IETF Standard	ISO Standard	IEEE Standard	Bluetooth SIG Standard	LoRa Alliance Standard	IEEE Standard	IETF Standard	Proprietary

The comparison table-1 is based on general characteristics of each protocol, and specific implementations may vary. Additionally, the suitability of a particular protocol for a given IoT application depends on various factors, such as the nature of the application, the available resources, and the constraints of the environment.

Security Attacks on IOT Networks

There are several types of security attacks that can be targeted towards IoT networks, some of which include [13], [14]:
1. Denial-of-service (DoS) attacks: This is a type of attack that floods the network with traffic, causing it to become unavailable or unresponsive.
2. Man-in-the-middle (MITM) attacks: This is an attack where the attacker intercepts communication between devices, allowing them to eavesdrop, modify or inject data into the communication.
3. Botnet attacks: This is a type of attack where a large number of devices are targeted with malware and controlled by the attacker to carry out attacks.
4. Ransomware attacks: This is a type of attack where the attacker locks the device or network, demanding a ransom in exchange for unlocking it.
5. Credential attacks: This is a type of attack where the attacker tries to obtain user credentials such as passwords or PINs to gain unauthorized access to the network.
6. Physical attacks: This is a type of attack where the attacker physically accesses the device or network to steal or manipulate data.

7. Malware attacks: This is a type of attack where the attacker infects the network with malicious software, allowing them to control or damage the network.
8. Distributed denial-of-service (DDoS) attacks: This is a type of attack where a large number of devices flood the network with traffic, causing it to become unavailable or unresponsive.
9. Zero-day exploits: This is an attack that takes advantage of a vulnerability in the software or firmware of IoT devices that is unknown to the manufacturer or developer.
10. Rogue device attacks: This is an attack where an unauthorized device is introduced into the network, allowing the attacker to gain access to the network or compromise its security.
11. Brute-force attacks: This is an attack where an attacker attempts to guess a user's password by trying every possible combination until the correct one is found.
12. Eavesdropping attacks: This is an attack where an attacker intercepts communication between devices, allowing them to eavesdrop, modify or inject data into the communication.
13. Sinkhole attack: a sinkhole attack is a type of cyber attack that can be targeted towards IoT networks, where an attacker hijacks a large number of devices and redirects their traffic to a malicious server controlled by the attacker, with the aim of collecting sensitive information or launching other types of attacks.
14. Sybil attack: a Sybil attack is a type of cyber attack that can be targeted towards IoT networks, where an attacker creates multiple fake IoT devices in the network to gain control or influence over the network, disrupt its operations, or steal sensitive information.
15. Wormhole attack: a wormhole attack is a type of cyber attack that can be targeted towards IoT networks, where an attacker creates a shortcut or "wormhole" between two remote locations in the network, bypassing the normal routing path and allowing the attacker to intercept and manipulate the network traffic.
16. HELLO flood: Hello flood attack is a type of DDoS attack that can be targeted towards IoT networks, where an attacker sends a large number of Hello messages to the network, overwhelming it with traffic and causing it to become unresponsive.
17. Acknowledgement spoofing: an acknowledgement spoofing attack is a type of cyber attack that can be targeted towards IoT networks, where an attacker sends fake ACK messages to the network, making it appear that a legitimate device has received and acknowledged a message, when in reality it has not.

III CONCLUSION AND FUTURE SCOPE

In this paper IOT based protocols and security attacks have been addressed. The study shows that security in IoT is challenged by device limitations and absence of standards, such as IoT-specific protocols and channel-based security measures. Despite the complexity involved, there are research prospects to explore the deployment of IDS in IoT, the development of energy-efficient cryptography methods that are suitable for the limited resources, and optimizing the available resources to improve security.

REFERENCES

[1] S. H. Shah and I. Yaqoob, “A survey: Internet of things (iot) technologies, applications and challenges,” in 2016 IEEE Smart Energy Grid Engineering (SEGE), 2016, pp. 381–385
[2] Atzori, L., Iera, A., & Morabito, G. (2010). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660. DOI: 10.1016/j.future.2013.01.010
[3] Faghih, F., Hejazi, M., & Hatzinakos, D. (2018). IoT Infrastructure: A Systematic Literature Review. IEEE Internet of Things Journal, 5(5), 3810-3823. DOI: 10.1109/JIOT.2018.2873247
[4] Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2017). IoT Security: A Comprehensive Survey. IEEE Internet of Things Journal, 4(6), 2836-2855. DOI: 10.1109/JIOT.2017.2760070

[5] Shelby, Z., Hartke, K., & Bormann, C. (2014). The Constrained Application Protocol (CoAP). RFC 7252. DOI: 10.17487/RFC7252
[6] Kim, H., Yoon, Y., & Hong, S. (2017). Lightweight IoT Protocol Stack: RPL and CoAP. Sensors, 17(9), 2088. DOI: 10.3390/s17092088
[7] Zhou, J., Wu, W., & Wang, J. (2015). Study on the Communication Protocols of IoT. International Journal of Distributed Sensor Networks, 11(1), 1-11. DOI: 10.1155/2015/189706
[8] Bhawarkar, D., Koli, N., & Patil, R. (2017). MQTT: A Review of Security Threats and Mitigation Techniques. International Journal of Computer Applications, 169(11), 1-5. DOI: 10.5120/ijca2017914063
[9] Verma, S., & Prasad, A. (2018). An analysis of security threats and countermeasures in AMQP protocol. Journal of Ambient Intelligence and Humanized Computing, 9(4), 1115-1128. DOI: 10.1007/s12652-017-0528-1
[10] Augustin, A., Yi, J., Clausen, T., & Townsley, W. M. (2016). A Study of LoRa: Long Range & Low Power Networks for the Internet of Things. Sensors, 16(9), 1466. DOI: 10.3390/s16091466
[11] Shelby, Z., & Bormann, C. (2012). 6LoWPAN: The Wireless Embedded Internet. John Wiley & Sons. DOI: 10.1002/9781119951438
[12] Meijerink, B., & Bentum, M. J. (2019). LoRa and Sigfox for long-range IoT: A comparative analysis. Sensors, 19(12), 2772. DOI: 10.3390/s19122772
[13] Alaba, F. A., Ayo, C. K., & Aderounmu, G. A. (2017). Internet of things security: A survey. Journal of Network and Computer Applications, 88, 10-28. DOI: 10.1016/j.jnca.2017.03.012
[14] Rezaei, H., Hashemi, S. M., & Mohammadi, M. (2018). A survey on security attacks and countermeasures in wireless sensor networks and Internet of Things. Journal of Network and Computer Applications, 107, 20-34. DOI: 10.1016/j.jnca.2018.02.005
SHRADHA EDUCATIONAL ACADEMY