Security Threats, Attacks, and Possible Countermeasures in Internet of Things

Shams Tabrez Siddiqui, Shadab Alam, Riaz Ahmad and Mohammed Shuaib

Abstract The idea to connect everything to anything and at any point of time is what vaguely defines the concept of Internet of Things (IoT). The concept of IoT is not only about providing connectivity but also facilitating interaction among these connected things. Though the term IoT was introduced in 1999 but has drawn significant attention during the past few years. The pace at which new devices are being integrated into the system will profoundly impact the world in a good way but also poses some serious threats with regard to security and privacy. IoT in its current form is susceptible to a multitudinous set of attacks. One of the greatest concerns of IoT is to provide security assurance for the data exchange because data is vulnerable to a number of attacks by the attackers at each layer of IoT. The IoT has layered structure, where each layer provides a service. The security vary from layer to layer as each layer serves a different purpose. The aim of this paper is to analyze the various security and privacy threats related to IoT. Furthermore, this paper also discusses numerous existing security protocols operating at different layers, potential attacks, and suggested countermeasures.

Keywords Internet of things · Attacks · Security · Threats · Protocols

S. T. Siddiqui · S. Alam · M. Shuaib
Department of Computer Science, Jazan University, Jazan, Saudi Arabia
e-mail: stabrezsiddiqui@gmail.com

S. Alam
e-mail: s4shadab@gmail.com

M. Shuaib
e-mail: talkshuaib@gmail.com

R. Ahmad (✉)
Department of Computer Science, Aligarh Muslim University, Aligarh, India
e-mail: riaz.ahmad.tech@gmail.com

M. L. Kolhe et al. (eds.), *Advances in Data and Information Sciences*,
Lecture Notes in Networks and Systems 94,
https://doi.org/10.1007/978-981-15-0694-9_5

1 Introduction

IoT emerged in the year 1999 with the introduction of Wireless Sensor Networks (WSN) and technologies like Radio-Frequency Identification (RFID). The concept behind the IoT is to connect everything to anything, anywhere, and at any moment of time. For making physical or virtual connections, it uses objects like sensors, actuators, etc. The success of IoT infrastructure and applications depends on IoT security. IoT collects the data from a vast geographical region using sensors and actuators [1].

The IoT is going to gain the attention of masses. The concept of IoT devices is not only about providing connectivity but also they need to be interactive. The need of hour is that they should deploy context-based interactions [2]. There will be billions of interconnectivity among the internet that will surely open doors for hackers and with that there will be a lot of security and privacy threats that will need immediate supervisions.

The objective of IoT technology is to provide interconnections between humans, things, and between humans and objects. In the IoT infrastructure, the sensors and objects are integrated for communications that can work successfully without human interventions. The sensors play an important role in IoT as these devices not only collect heterogeneous data but also monitors the data with diversity and is quite intelligent and dynamic in nature [3, 4]. The major IoT principles include confidentiality, authentication, availability, heterogeneity, lightweight solutions, key management, policies, and integrity.

IoT has a layered structure where each layer provides a service. Usually, the IoT architecture is categorized in three layers, namely, application, network, and perception layer. The security issues like privacy, authorization, verification, access control, system configuration, information storage, and management that are the real challenges of the IoT infrastructure [5, 6]. The security needs vary from layer to layer as each layer serves a different purpose [5]. Undoubtedly, to make IoT a reality the security issues need to be resolved. There are two types of security challenges, namely, technological and security challenges. The technological challenges include wireless technologies and the distributed nature of the IoT. The challenges related to authentication and confidentiality included in the security [7].

This paper discusses the protocols present on different IoT layers and identify the security threats at each layer. Different security issues and its countermeasures have been discussed in detail. The objective of this paper is to enlighten the essential security protocols of IoT that obliging for the prevention of harmful threats.

2 IoT Architecture

IoT has a three-layered architecture. The three layers are as follows:

Table 1 Different protocols that are present on different layers

IoT layers	Protocols
Application layer	CoAP, DDS, MQTT, SMQTT, AMQP
Network layer	6LoWPAN, RPL, CORPL, CARP, 6TISCH
Perception layer	LTE-A, Z-Wave, ZigBee smart, DASH7, 802.11AH

- The Application Layer,
- The Network Layer, and
- The Perception Layer.

The Application Layer: The main aim of the application layer is to deliver specific services to its users [8]. It defines numerous applications of IoT, viz., smart home, health, cities where it can be deployed.

The Network Layer: This layer is most prone to attacks, it aggregates data from existing infrastructures and transmits the data to other layers. It processes the sensor data. The major security issues usually related to authentication and integrity of data that is being transmitted [9].

The Perception Layer: This is the physical layer, even known as the lowest layer of the IoT architecture and reflected as a brain of the three-layered architecture. The sensing devices like the sensors and actuators are present at this layer. This layer is also known as the sensor layer [10, 11] (Tables 1 and 2).

3 Security Requirements

IoT infrastructure consists of a lot of personal information such as name, date of birth, locations, etc. Therefore, we need to provide strict measures to protect the data and tackle privacy risks. In order to overcome the security challenges, the layered structure is adopted. The basic security properties that need to be implemented are confidentiality, authenticity, integrity, and availability. There are a number of other security requirements that are derived from the basic security requirements such as scalable, IP Protocol-Based IoT, Heterogeneous IoT, and Lightweight Security.

4 IoT Security Threats

The threats can broadly be classified into three categories. The categories are capture, disrupt, and manipulate. The capture threat means capturing information or system without authorization. The capture threats are such threats that are designed to gain access of information that is either logical or physical on a system. The disrupt

Table 2 Application, network, and perception layer protocols

PROTOCOLS	PURPOSE
CoAP	Constrained application protocol (CoAP) is designed in such a way that it enables the low-power sensors to make usage of restful services. It is very much similar to HTTP and is built upon the UDP instead of TCP packets [12]
DDS	Data distribution service (DDS) provides an excellent quality of service that can have scalability with excessive overall performance and reliability that suits the IoT and M2M communication [12]
MQTT	Message Queue Telemetry Transport Protocol (MQTT) facilities the embedded connectivity between applications and the middlewares at one side whereas the networks and communications on the other side [13]
SMQTT	Secure Message Queue Telemetry Transport Protocol (SMQTT), the message is encrypted before delivering to multiple nodes in the network [14]
AMQP	Advanced Message Queuing Protocol is a software layer protocol having three additives, namely, exchange, message queue, and binding. This protocol is generally message-oriented for middleware environment [15]
6LoWPAN	Wireless sensor network is one of the applications of IPv6 Low-Power Wireless Personal Area Network (6LoWPAN) system, uses it while sending data as a packet. It provides huge variety of network connected to internet providing end-to-end services [16]. The specification supports different length addresses, low bandwidth, different topologies including star or mesh, power consumption, low cost, scalable networks, mobility, unreliability, and long sleep time
RPL	Routing Protocol for wireless network with Low-Power consumption having Lossy Networks (RPL) supports one-to-one communication [16]. It can quickly create network routes, adapt topology in an efficient way, share routing knowledge but susceptible to packet loss
CORPL	It is a routing protocol for cognitive radio enabled AMI network? An extension of RPL designed for the cognitive networks but with two new modification that uses DODAG topology generation [17]
CARP	Channel-Aware Routing Protocol (CARP) is a distributed routing protocol designed for light-weighted packets in IoT. Therefore, it is used for acoustic communication under the water [18]
6TiSCH	IPv6 time-slotted channel hopping (6TiSCH) working group in IETF is developing standards to allow IPv6 to pass through TSCH mode of IEEE 802.15.4e data links [19]. TSCH demonstrate end-to-end reliability. This essentially a MAC layer that offers globally synchronized mash network of sleepy node and is also defined as minimal configuration
LTE-A	Long-Term evolution advanced (LTE-A) is an agglomeration of cellular network. As compared to other cellular networks it is one of the most scalable and lower cost protocol [20]

(continued)

Table 2 (continued)

PROTOCOLS	PURPOSE
Z-WAVE	Z-Wave is a low cost and low-power MAC protocol that design aimed specifically for home automation [21]
ZigBee Smart Energy	An enhancement to the customary ZigBee is ZigBee IP or Smart which is designed for the substantial range of IoT applications including smart homes, healthcare systems, and for remote controls. It supports numerous topologies including star, peer-to-peer or cluster tree [22]
DASH7	DASH7 is a wireless communication protocol for active RFID specifically designed for scalable, long-range outdoor coverage with higher data rate. It provides low cost and light-weighted solutions [23]
IEEE 802.11 AH	IEEE 802.11ah is a wireless networking protocol with low energy capable communication standard [24]

Table 3 The description of threats at each layer

IoT layers	Threats
Application layer	Malicious code attacks, Tampering with node-based applications, Inability to receive security patches, Hacking into the smart meter/grid, Phishing Attack, Malicious Virus/worm, Malicious Scripts, Remote configuration, Mis-configuration, Security management, Management system
Network layer	DoS attack, Gateway attacks, Unauthorized access, Storage attacks, Injecting fake information, Spoofing attacks, Sinkhole attacks, Wormhole attacks, Man-in-the-Middle attack, Routing attacks, Sybil attacks, Unauthorized access
Perception layer	Wireless Sensor Networks (WSN), Eavesdropping, Repudiation, Noise in data, Privacy threats services abuse, RFID, Service information Manipulation, Sniffing attacks, Identity masquerade, Replay attack

threat means denying access or destroying a system. The manipulated threat means manipulating time series data, identity, or the data (Table 3).

5 IoT Challenges

Due to the vast scale of IoT infrastructure with a huge number of devices involved in developing a successful IoT application is not an easy task and have to face a lot of challenges. Some of the challenges are, namely, mobility, reliability, availability Identification, scalability, data integrity, management, energy management, interoperability, and security and privacy.

Mobility: It is one of the essential issues of the IoT paradigm. As IoT devices move freely from one network to another, therefore, movement detection is important to monitor the device location and respond to the topology that changes accordingly due to which layer of complexity escalate to another level [25].

Reliability: Reliability is a very critical requirement in the application that requires all the emergency responses correctly otherwise, it will be a huge disastrous scenario. In IoT applications, data collection, communication should be fast and highly reliable [25].

Scalability: Other challenges of IoT application is scalability, where enormous number of devices are connected to a network, therefore, the protocols must have efficient extensible services to meet the IoT devices requirements [26].

Management: Managing a vast number of devices and keeping track of their failures, configurations, and performances in the network is an immense challenge [26].

Energy management: In IoT devices, energy is required still not adequately met. Some routing protocols at an early stage of development supports low power communication but to make IoT devices more power efficient, Green technology must be employed [25].

Availability: Availability means the service subscriber provides the service anytime and anywhere for the service subscribers. Software service provided to anyone who is authorized to, whereas the hardware availability means easy to access and are compatible with IoT functionality and protocols.

Interoperability: Huge number of heterogeneous devices and protocols work with each other. This becomes a challenging task due to the number of IoT devices using various platforms [25].

Identification: To provide innovative services, the IoT devices are interconnected with numerous objects, and hence, an efficient naming and identity managing system is required to specify the object [26].

Data Integrity: IoT devices are heterogeneous in nature, therefore, they have to deal with big amount of data. Handling big data is very crucial as overall the performance is directly proportional to the features of data management services. Became more complicated when data integrity features are considered, it also affects the QoS, Privacy, and Security related issues specifically on outsourced data [25, 26].

6 Counter Measures

The countermeasures that can be taken are the authentication measures, establishment of trust, and acceptance of federated architecture awareness of security issues (Table 4).

Table 4 The countermeasure of threats at each layer

IoT Layers	Protocols	Threats	Countermeasures	Countermeasures description
Application layer	CoAP, DDS, MQTT, SMQTT, AMQP	Malicious code attacks	Runtime type checking, Firewall checks	Seem to do runtime type checking, immune for all ill-typed code tried. At runtime, the firewall checks have to be done
		Tampering with node-based applications	Physically secure design	Physically secure designing of devices should not be of high quality and unreliable [27]
		Inability to receive security patches	Evading security risks with regular patching and support services	
		Hacking into the smart meter and kill the grid	Security Frameworks to Prevent from Hacking the Grid	
		Malicious injection	Custom FileZilla as the FTP client	The credentials of the websites stored in plain text by FileZilla
		Remote configuration	Configuring and managing VPNs	NCP engineering offers inclusive software that designed for the clients indispensable to control large networks
		Application security	Web Application Scanner	Discovery of various threats which is present on the front end of web [28]
		Security management	Security management is the identification of an organization's assets followed by the development, documentation, and implementation of policies and procedures for protecting these assets	
		Data security	Fragmentation redundancy scattering	Data on cloud splits and apportions to various fragments for the storage in servers [29]
		Shared resources	Holomorphic encryption	Ciphertext allowed to reckon immediately without decryption [27]
		Mis-configuration	This attack can occur at any level of an application stack including the platform, application server, web server, database, and framework [30]	

(continued)

Table 4 (continued)

IoT Layers	Protocols	Threats	Countermeasures	Countermeasures description
Network layer	6LoWPAN, RPL, CORPL, CARP, 6TISCH	DoS attack	This can be handled by assuring that resources are committed to a client only after proper authentication, utilization of proxy servers with sufficient resources, protocol scrubbing (to remove protocol uncertainties which can be misused for attacks)	
		Gateway attacks	Blocking spyware at the Network gateway	Block against viruses, spam, and intruders, organizations deploy countermeasures at the network gateway and again in individual client systems
		Unauthorized access	Device authentication	Without any authentication, the device cannot enter or connect with other nodes in the IoT system
		Storage attacks	In case of physical security weaknesses, the attackers can effortlessly access the storage medium via disassemble the device	
		Injecting fake information	Injecting fake routing control packets in the network	
		Spoofing attacks	IPsec will significantly cut down on the risk of spoofing	Use authentication based on the key exchange between the machines on your network; Enable encryption sessions on your router so that trusted hosts that are outside your network can securely communicate with your local hosts
		Sinkhole attacks	Security aware and ad hoc routing	Stops inside attacks from the network of IoT, use key management, authentication, and geographical routing protocols, and drop adversary from the network
		Wormhole attacks	Routing Protocol (AODV and DSR)	Stratagem the packet LEACH techniques for detecting and thus defending against said attacks

(continued)

Table 4 (continued)

IoT Layers	Protocols	Threats	Countermeasures	Countermeasures description
		Man in the Middle attack	Secure/Multipurpose Internet Mail Extensions, or S/MIME; Authentication Certificates	Hackers will never go away, but one thing you can do is make it virtually impossible to penetrate your systems by implementing Certificate-Based Authentication for all employee machines and devices
		Routing information attacks	Encrypting routing tables	was identifies different security issues on the web by encryption process in rout
		Sybil attacks	Authentication and encryption preclude from outsider attack, Privilege Attenuation, Economic Incentives, public-key cryptography preclude from insider attacks [25, 31]	
		Unauthorized access	Two-factor authentication, IP White listing	
Perception Layer	LTE-A, Z-Wave, Zigbee smart, DASH7, 802.11ah	RF interface on RFID	Device authentication	Before sending and receiving of data from a new physical device the device should authenticate itself
		Jamming node in Wireless Sensor Networks (WSN)	IPsec Security channel	Can be circumvented by stratagem different paths for routing [25, 31]
		Eavesdropping	Session Keys protect NPDU from Eavesdropper [31]	
		Sniffing attacks	Sniffer detection tools like ARP Watch, PromiScan, Anti-Sniff, Pro detect	Applications using secure protocols viz., HTTPS, SFTP, SSH. If obligatory than VPN can be used to provide the users with secure access
		Noise in data		
		Privacy threats	RFID	

(continued)

Table 4 (continued)

IoT Layers	Protocols	Threats	Countermeasures	Countermeasures description
		Services abuse		
		Identity masquerade	verify identity; strong password	Generally, a unique user ID is assigned to each user, but passwords are something you must set (or change) by yourself. If your User ID and Password are compromised or stolen, somebody else might use them to access your system or other systems, masquerading as a legitimate user
		Service information manipulation		
		Repudiation	Create secure audit trails; Use digital signatures	
		Replay attack	Timestamps, one-time passwords, and challenge-response cryptography [25]	

7 Conclusion

IoT has recently emerged as an important research topic. Due to emerging technology attackers take advantages of the IoTs great potential to threaten users privacy, security, and wide variety of attacks. Therefore, it is essential to focus on the security parameters and heeded toward giving new feasible solutions to block all possible threats and vulnerabilities to IoT. This paper presents a comprehensive overview of security threats and attacks on IoT. Application, network and perception layer protocols with purpose been discussed. In addition, this paper suggested several countermeasures against identified security threats of each layer.

A lot more need to happen in near feature in the area of IoT applications. This IoT field will definitely mature the impact of human life in inconceivable ways over the next decades. As IoT is going to play an indispensable part in our lives, steps should be taken to ensure the security and privacy of the users.

Future work involves finding alternative solutions for attacks that are less complex and less time-consuming. Future research involves development of protocols and finds ways to overcome security threats and attacks.

References

1. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.
2. Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. *Computer, 9,* 51–58.
3. Horrow, S., & Sardana, A. (2012). Identity management framework for cloud based internet of things. In *Proceedings of the First International Conference on Security of Internet of Things* (pp. 200–203). ACM.
4. Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers*, *17*(2), 261–274.
5. Aazam, M., St-Hilaire, M., Lung, C. H., & Lambadaris, I. (2016). PRE-Fog: IoT trace based probabilistic resource estimation at Fog. In *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)* (pp. 12–17). IEEE.
6. Jiang, H., Shen, F., Chen, S., Li, K. C., & Jeong, Y. S. (2015). A secure and scalable storage system for aggregate data in IoT. *Future Generation Computer Systems, 49,* 133–141.
7. Li, S., Tryfonas, T., & Li, H. (2016). The Internet of Things: A security point of view. *Internet Research, 26*(2), 337–359.
8. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347–2376.
9. Pongle, P., & Chavan, G. (2015). A survey: Attacks on RPL and 6LoWPAN in IoT. In *2015 International Conference on Pervasive Computing (ICPC)* (pp. 1–6). IEEE.
10. Tsai, C. W., Lai, C. F., & Vasilakos, A. V. (2014). Future Internet of Things: Open issues and challenges. *Wireless Networks, 20*(8), 2201–2217.
11. Sethi, P., & Sarangi, S. R. (2017). Internet of things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*.
12. Karagiannis, V., Chatzimisios, P., Vazquez-Gallego, F., & Alonso-Zarate, J. (2015). A survey on application layer protocols for the internet of things. *Transaction on IoT and Cloud Computing, 3*(1), 11–17.

13. Locke, D. (2010). Mq telemetry transport (mqtt) v3. 1 protocol specification. *IBM developer Works Technical Library*.
14. Singh, M., Rajan, M. A., Shivraj, V. L., & Balamuralidhar, P. (2015). Secure mqtt for internet of things (iot). In *2015 Fifth International Conference on Communication Systems and Network Technologies* (pp. 746–751). IEEE.
15. OASIS, O. S. (2012). OASIS Advanced Message Queuing Protocol (AMQP) Version 1.0. Burlington, MA, USA: OASIS.
16. Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., & Alexander, R. (2012). RPL: IPv6 routing protocol for low-power and lossy networks (No. RFC 6550).
17. Aijaz, A., & Aghvami, A. H. (2015). Cognitive machine-to-machine communications for Internet-of-Things: A protocol stack perspective. *IEEE Internet of Things Journal, 2*(2), 103–112.
18. Zhou, Z., Yao, B., Xing, R., Shu, L., & Bu, S. (2016). E-CARP: An energy efficient routing protocol for UWSNs in the internet of underwater things. *IEEE Sensors Journal, 16*(11), 4072–4082.
19. Dujovne, D., Watteyne, T., Vilajosana, X., & Thubert, P. (2014). 6TiSCH: Deterministic IP-enabled industrial internet (of things). *IEEE Communications Magazine, 52*(12), 36–41.
20. Hasan, M., Hossain, E., & Niyato, D. (2013). Random access for machine-to-machine communication in LTE-advanced networks: Issues and approaches. *IEEE Communications Magazine, 51*(6), 86–93.
21. Yassein, M. B., Mardini, W., & Khalil, A. (2016). Smart homes automation using Z-wave protocol. In *2016 International Conference on Engineering & MIS (ICEMIS)* (pp. 1–6).
22. Wang, C., Jiang, T., & Zhang, Q. (2016). *ZigBee® network protocols and applications*. Auerbach Publications. 604 pp.
23. Cetinkaya, O., & Akan, O. B. (2015). A DASH7-based power metering system. In *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)* (pp. 406–411). IEEE.
24. https://standards.ieee.org/standard/802.11ah-2016.html.
25. Salman, T., & Jain, R. (2017). Networking Protocols and Standards for Internet of Things. Wiley.
26. Triantafyllou, A., Sarigiannidis, P., & Lagkas, T. D. (2018). Network protocols, schemes, and mechanisms for internet of things (iot): Features, open challenges, and trends. *Wireless Communications and Mobile Computing*.
27. Abomhara, M., & Køien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. In *2014 International Conference On Privacy And Security In Mobile Systems (Prisms)* (pp. 1–8). IEEE.
28. Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh, S. (2014). IoT security: Ongoing challenges and research opportunities. In *2014 IEEE 7th International Conference On Service-Oriented Computing And Applications* (pp. 230–234). IEEE.
29. Migault, D., Palomares, D., Herbert, E., You, W., Ganne, G., Arfaoui, G., & Laurent, M. (2012). E2e: An optimized ipsec architecture for secure and fast offload. In *2012 Seventh International Conference on Availability, Reliability and Security* (pp. 365–374). IEEE.
30. https://support.portswigger.net/customer/portal/articles/1965728-using-burp-to-test-for-security-misconfiguration-issues.
31. El Mouaatamid, O., Lahmer, M., & Belkasmi, M. (2016). Internet of Things Security: Layered classification of attacks and possible Countermeasures. *Electronic Journal of Information Technology*, (9).