SECURITY& PRIVACY THREATS, ATTACKS AND COUNTERMEASURES IN INTERNET OF THINGS

Faheem Masoodi[1]Shadab Alam[2] and Shams Tabrez Siddiqui[2]

[1]Department of Computer Science, University of Kashmir, J&k, India
[2]Department of Computer Science, Jazan University, KSA

ABSTRACT

The idea to connect everything to anything and at any point of time is what vaguely defines the concept of the Internet of Things (IoT). The 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 severe queries about security and privacy. IoT in its current form is susceptible to a multitudinous set of attacks. One of the most significant concerns of IoT is to provide security assurance for the data exchange because data is vulnerable to some attacks by the attackers at each layer of IoT. The IoT has a layered structure where each layer provides a service. The security needs vary from layer to layer as each layer serves a different purpose. This paper aims to analyze the various security and privacy threats related to IoT. Some attacks have been discussed along with some existing and proposed countermeasures.

KEYWORDS

Internet of Things, privacy, attacks, security, threats, protocols.

1. INTRODUCTION

Kevin Ashton in 1999 coined the term 'Internet-of-Things (IoT)' [1] and was primarily used to describe how IoT can be created by "adding radiofrequency identification and other sensors to everyday objects." Today the term IoT encompasses a set of heterogeneous devices that are connected via some communication protocols and sensors, which enable us to locate, identify and operate upon these devices.

The 'things' in IoT are the entities that are involved in communication among themselves and with the environment in which they exist and are responsible for generating large amounts of data and information. For making physical or virtual connections, it uses objects like sensors, actuators,etc. The success of IoT infrastructure and applications depends on IoT security. The IoT collects the data from a vast geographical region using sensors [1].

The Cisco Internet Business Solutions Group (IBSG) has come up with a ballpark figure of 50 billion IoT devices by 2020,and the rationale for this massive number is the numerous and attractive services provided by IoT. Communication protocols that played a vital role in the emergence of IoT include Wireless Sensor Networks (WSN), Radio-Frequency Identification (RFID), Internet protocols and mobile communications. The concept of IoT devices is not onlyabout providing connectivity but also interaction among themselves. The need of the hour is that they should deploy context-based interactions [2]. There will be billions of devices interacting among each other over the internet, that will surely open doors for hackers, and with

that, there will be a lot many security threats that will need immediate supervisions. In the IoT infrastructure, the sensors and objects are integrated for communications that can work successfully without human interventions. The sensors play an essential role in the IoT as these are devices that not only collect heterogeneous data but also monitor it [3][4].

The goal of IoT is to provide a network infrastructure for interactions between sensor devices and other humans and objects. The IoT has a layered structure where each layer provides a service. The security needs vary from layer to layer as each layer serves a different purpose [5]. A considerable number of issues need to be addressed with regard to the IoT infrastructure. The reasons being the following:

- Nature of smart objects
- Usage of standard protocols
- The bidirectional flow of information

The security issues like privacy, authorization, verification, access control, system configuration, information storage, and management are the real challenges of the IoT infrastructure [6]. Undoubtedly, to make IoT a reality, the security issues need to be resolved. IoT is the future generation internet.

The two types of challenges that we need to focus on are technological and security challenges.

The technical difficulties include wireless technologies and the distributed nature of the IoT while as the problems related to authentication and confidentiality are involved in the security[7].The major IoT principles include confidentiality, authentication, availability, heterogeneity, lightweight solutions, key management, policies, and integrity

2. IOT ARCHITECTURE

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

- The Application Layer
- The Network Layer
- The Perception Layer

The Application Layer: The main aim of the application layer is to provide services to its users[8].

The Network Layer: The layer that is most prone to attacks is the network layer as it aggregates data from existing infrastructures and it transmits that data to other layers. The primary security issues are related to the authentication and integrity of data that is being transmitted [9].

The Perception Layer: The lowest layer of the IoT architecture and also the brain of the three-layered architecture. It is the physical layer.The sensing devices like the sensors are present on this layer. It is also known as sensors layer [10].

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

Table 1. Different protocols that are present on different layers

PROTOCOLS	PURPOSE
CoAP	CoAP is designed in such a way that it enables the low-power sensors to make usage of restful services It is built upon the UDP instead of the TCP that is commonly used in HTTP.
DDS	It provides an excellent quality of service levels and reliability that suits the IoT and M2M communication.
MQTT	It facilities the embedded connectivity between applications and the middleware's at one side and networks and communications on the other
SMQTT	In this one message is encrypted but delivered to multiple other nodes.
AMQP	In this, the broker is divided into two main components that are exchange and queues.
6LoWPAN	6LoWPAN is designed to work with variant length addresses, various network topologies including mesh and star, low bandwidth, scalable networks, mobility, and low cost
RPL	Routing Protocol for Low-Power and Lossy Networks (RPL) supports data link protocol.
CORPL	An extension of RPL is CORPL or cognitive RPL, which is designed for the cognitive networks and uses DODAG topology generation.
CARP	A distributed routing protocol is designed for the underwater Communication. It has lightweight packets.
6TiSCH	A 6TiSCH working group in IETF is developing standards to allow IPv6 to pass through Time- Slotted Channel Hopping (TSCH) mode of IEEE 802.15.4e data links.
LTE-A	LTE-A is a scalable, lower- cost protocol as compared to other cellular protocols.
Z-WAVE	Z-Wave is a low-power MAC protocol that is designed for home automation.
Zigbee Smart Energy	It is designed for a broad range of IoT applications including Smart homes, remote controls, and healthcare systems. It supports a wide star, peer-to-peer or cluster-tree topologies.
	The objective is to support scalable networks with more extended distance coverage at higher data rates.
IEEE 802.11 AH	IEEE 802.11ah is a low energy version of the original IEEE 802.11 wireless medium access standard.

Table 2. Application, network and perception layer protocols [11-23].

3. SECURITY REQUIREMENTS

The security and privacy issues have emerged as one of the primary concern in IoT implementation. Fig. 1 shows the web search of these terms measured by Google search trends since Jan 2004. It is clear that since 2014, search volume is increasing for both the terms primarily because of the large scale integration of IoT devices during last five years and increasing concern among the users about the confidentiality and privacy of their information contained in the systemWhile as Privacy includes the concealment of personal information as well as the ability to control what happens with this information [27][29], IoT security is concerned with safeguarding "things" in the Internet of things. IoT systems are prone to security attacks for a variety of reasons including the wireless communication between devices, physical access to objects, the constrained capacity of smart devices and openness of the system [30]. Broken devices or permanent failures of such devices provide vulnerabilities and can,therefore be exploited by potential attackers. A typical example of such devices can be RFID tags.

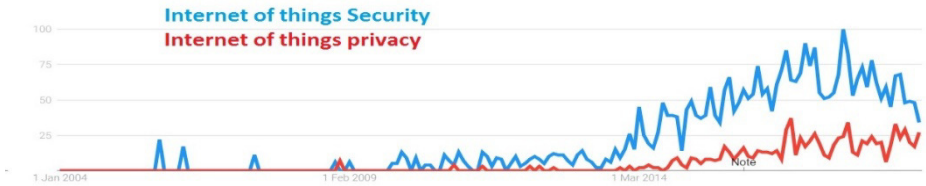

Fig. 1. Google search trends since 2004 for terms IOT Security, IOT Privacy

What makes privacy an essential IoT requirement lies in the anticipated IoT application domains and the technologies used. IoT adoption is harnessed due to lack of adequate measures for ensuring the privacy of information in variant IoT application fields like patient's remote monitoring, energy consumption control, traffic control, smart parking system, inventory management, and production chain,etc. [31]. Additionally, the adoption of wireless communication medium for data exchange can lead to a potential risk of privacy violation as exchanges over such medium can expose the underlying system to multiple attacks. Under these circumstances, security and privacy represent a real research challenge that may restrict IoT development. In an attempt to address these security and privacy concerns, we need to provide strict measures to protect data and tackle privacy risks. The underlying security properties that need to be implemented are confidentiality, authenticity, integrity and availability. Some other security requirements are derivedsuch as scale, IP Protocol-Based IoT, Heterogeneous IoTand Lightweight Security.

4. IOT SECURITY THREATS AND ATTACKS

The Internet of things offers many applications that are of substantial value to the user but at the same time can expose the user to unprecedented security threats and challenges. Much of this threat comes from the fact that the devices connected in an IoT network share some level of trust and exchange information without performing any malware tests. 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 to information that is either logical or physical on a network. The disrupt threat means denying access or destroying a system.The manipulate threat means manipulating time series data or identity. Multiple security vulnerabilities exist in the current system with the potential to result in security concerns including Insecure network services and software/firmware, lack of transport encryption, insecure cloud and mobile interface, insufficient security configurability and poor physical security, insufficient authorization/authentication, insecure web services and privacy concerns [32][33].

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 , Misconfiguration, 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	RFID, Wireless Sensor Networks (WSN), Eavesdropping, Sniffing Attacks, Noise in data, Privacy threats Services abuse, Identity masquerade ,Service information Manipulation, Repudiation, Replay attack

5. COUNTERMEASURES (EXISTING AND PROPOSED)

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

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	Appear to do runtime type checking, making them immune to all ill-typed code we tried. Firewall checks have to be done at runtime
		Tampering with node-based applications	Physically secure design	Physically Secure Designing of devices should not be changeable and not be of high quality[26]
		Inability to receive security patches	Avoiding security risks with regular patching and support services	
		Hacking into the smart meter/grid	Security Frameworks to Prevent Hacking The Grid	
		Malicious injection	Use FileZilla as the FTP client.	You must know that FileZilla store the credentials of your websites in plain text
		Remote configuration	Configuring and managing. VPNs	NCP engineering provides a software VPN platform the solution that is designed for an organization that requires control over large networks.
		Application security	Web Application Scanner	Discovery of various threats which is present on the front end of web [24]
		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 is splits and allocates in to various fragments for storage in servers [25].
		Shared resources	Holomorphic encryption	Cipher text is allowed to compute immediately without decryption [26]
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 enters or connect with other node in the IOT system.
		Storage Attacks	Physical security weaknesses are present when an attacker can disassemble a device to easily access the storage medium and any data stored on that medium.	
		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 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 and the adversary is dropped from the network.
	Wormhole Attacks	Routing Protocol	Routing protocol is used to produce the multiple paths between the sender and receiver and checks the presence of route. Physical monitoring of Field devices and regular monitoring of network using Source Routing. Monitoring system may use packet leach techniques.
	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 web by encryption process in rout
	Sybil Attacks	Trusted Certification, Resource Testing, Recurring Fees, Privilege Attenuation, Economic Incentives, Location/Position Verification, Received Signal Strength Indicator (RSSI)–based scheme and Random Key Pre distribution. [28]	

		Unauthorized Access		
Perception smart, Layer	LTE-A, Z-Wave, Zigbee DASH7, 802.11ah	RF interface on RFID	Device authentication	A new Physical device before sending and receiving of data the device should authenticate itself
		Jamming node in Wireless Sensor Networks (WSN)	IPsec Security channel	Node tempering and eavesdropping can be stopped by changeable and not be of high quality [28]
		Eavesdropping	Session Keys protect NPDU from Eavesdropper	
		Sniffing Attacks	sniffer detection tools like ARP Watch, Promiscan, Anti-Sniff, Prodetect	
		Noise in data		
		Privacy threats	RFID	
		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 [28]	

6. CONCLUSIONS

The field of IoT is still considered to be in its nascent stage and the technologies employed have considerable scope to progress. Security and privacy pose a very serious challenge to the researches and hinders the growth of IoT. Due to the fact that IoT is an emerging technology, attackers take advantage of the underlying potential to threaten theuser's privacy, security using

wide variety of attacks. This paper presents the comprehensive overview of security threats and attacks on IoT. Countermeasures of the security threats and attacks deliberated with the detail description. The future work involves finding alternative solutions for attacks that are less complex and less time consuming. The future research involves development of protocols and find ways to overcome security threats and attacks.

7. FUTURE WORK

The IoT is developing at a very rapid pace, and successful growth of IoT is only possible ifwe address the security and privacy challenges related to the internet of things. A secure IoT paradigm is possible only with the redressal of issues like 5g protocols, key and identity management, fault tolerance, trust & group management and end-to-end security. As highlighted in this paper, work needs to done in the areas of IoT architecture, finding alternative solutions for attacks that are less complex in terms of time and other resources. Moreover, policies need to be devised concerning regulations, trust management, legal framework, and device security at the manufacturer's end.

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (IoT): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.

[2] Roman, R., Najera, P., Lopez, J., 2011. Securing the internet of things. Computer 44 (9), 51_58.

[3] Horrow, S., and Anjali, S. (2012). Identity Management Framework for Cloud-Based Internet of Things. SecurIT ’12 Proceedings of the First International Conference on Security of Internet of Things, 200– 203. 2012

[4] Whitmore, A., Agarwal, A., and Da Xu, L. (2014). 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., and Lambadaris, I. (2016). PRE-Fog: IoT trace based probabilistic resource estimation at Fog. 2016 13th IEEE Annual Consumer Communications and Networking Conference (CCNC), 12– 17.

[6] Jiang, H., Shen, F., Chen, S., Li, K. C., and 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., and Li, H. (2016). The Internet of Things: a security point of view. Internet Research, 26(2), 337– 359.

[8] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys Tutorials, 17(4):2347–2376, Fourth quarter 2015.

[9] Pongle, P., and Chavan, G. (2015). A survey: Attacks on RPL and 6LoWPAN in IoT. 2015 International Conference on Pervasive Computing: Advance Communication Technology and Application for Society, ICPC 2015, 0(c), 0–5.

[10] Tsai, C.-W., Lai, C.-F., and Vasilakos, A. V. (2014). Future Internet of Things: open issues and challenges. Wireless Networks, 20(8), 2201–2217.

[11] V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, "A survey on application layer protocols for the internet of things," Transaction on IoT and Cloud Computing, vol. 3, no. 1, pp. 11-17, 2015

[12] D. Locke, "MQ telemetry transport (MQTT) v3. 1 protocol specification," IBM Developer Works Technical Library, 2010, http://www.ibm.com/developerworks/webservices/library/ws-mqtt/index.html

[13] M. Singh, M. Rajan, V. Shivraj, and P. Balamuralidhar, "Secure MQTT for the Internet of Things (IoT)," in Fifth International Conference on Communication Systems and Network Technologies (CSNT 2015), April 2015, pp. 746-751.

[14] OASIS, "OASIS Advanced Message Queuing Protocol (AMQP) Version 1.0," 2012, http://docs.oasis-open.org/amqp/core/v1.0/os/amqp-core-complete-v1.0-os.pdf

[15] T. Winter, et al., "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," IETF RFC 6550, Mar. 2012, http://www.ietf.org/rfc/rfc6550.txt

[16] A. Aijaz and A. Aghvami, "Cognitive machine-to-machine communications for internet-of-things: A protocol stack perspective," IEEE Internet of Things Journal, vol. 2, no. 2, pp. 103-112, April 2015,

[17] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=7006643

[18] Z. Zhou, B. Yao, R. Xing, L. Shu, and S. Bu, "E-CARP: An energy-efficient routing protocol for UWSNs on the internet of underwater things," IEEE Sensors Journal, vol. PP, no. 99, 2015, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7113774

[19] D. Dujovne, T. Watteyne, X. Vilajosana, and P. Thubert, "6TiSCH: Deterministic IP-enabled industrial internet (of things)," IEEE Communications Magazine, vol. 52, no.12, pp. 36-41, December 2014, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6979984

[20] M. Hasan, E. Hossain, D. Niyato, "Random access for machine-to-machine communication in LTE-advanced networks: issues and approaches," in IEEE Communications Magazine, vol. 51, no. 6, pp.86-93, June 2013, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6525600

[21] Z-Wave, "Z-Wave Protocol Overview," v. 4, May 2007, https://wiki.ase.tut.fi/courseWiki/imges/9/94/SDS10243_2_Z_Wave_Protocol_Overview.pdf

[22] ZigBee Standards Organization, “ZigBee Specification,” Document 053474r17, Jan 2008, 604 pp., http://home.deib.polimi.it/cesana/teaching/IoT/papers/ZigBee/ZigBeeSpec.pdf

[23] O. Cetinkaya and O. Akan, "A dash7-based power metering system," in 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Jan 2015, pp. 406-411, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=7158010

[24] Zhang, Zhi-Kai, et al. ”IoT security: ongoing challenges and research opportunities.” Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on. IEEE, 2014.

[28] D. Migault, D. Palomares, E. Herbert, W. You, G. Ganne, G. Arfaoui, and M. Laurent, “E2E: An Optimized IPsec Architecture for Secure And Fast Offload,” in Seventh International Conference on Availability, Reliability and Security E2E: 2012.

[26] Abomhara, Mohamed, and Geir M. Køien. ”Security and privacy in the Internet of Things: Current status and open issues.” Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on. IEEE, 2014.

[27] B. L. Suto, “Analyzing the Accuracy and Time Costs of Web Application Security Scanners,” San Fr., no. October 2007, 2010.

[28] O. El Mouaatamid, M. LahmerInternet of Things security: layered classification of attacks and possible countermeasures Electron J (9) (2016).

[29] Seda F. Gürses/Bettina Berendt/Thomas Santen, Multilateral Security Requirements Analysis for Preserving Privacy in Ubiquitous Environments, in Bettina Berendt/Ernestina Menasalvas (eds), Workshop on Ubiquitous Knowledge Discovery for Users (UKDU '06), at 51–64;

[30] Stankovic, J. (2014). Research directions for the internet of things.IEEE Internet of Things Journal, 1(1), 3–9

[31] Sicari, Sabrina, et al. "Security, privacy and trust in the Internet of Things: The road ahead." Computer Networks76 (2015): 146-164.

[32] https://www.cso.com.au/article/575407/internet-things-iot-threats-countermeasures/ Accessed on 15-03-2019

[33] Bokhari, Mohammad Ubaidullah, and Faheem Masoodi. "Comparative analysis of structures and attacks on various stream ciphers." Proceedings of the 4th National Conference. 2010.