IoT Threats and Attacks

Subjects: Others

Contributor: Amitkumar V. Jha

The Internet of Things (IoT) plays a vital role in interconnecting physical and virtual objects that are embedded with sensors, software, and other technologies intending to connect and exchange data with devices and systems around the globe over the Internet. With a multitude of features to offer, IoT is a boon to mankind, but just as two sides of a coin, the technology, with its lack of securing information, may result in a big bane. It is estimated that by the year 2030, there will be nearly 25.44 billion IoT devices connected worldwide.

Internet of Things security threats privacy vulnerabilities Blockchain

1. Introduction

We live in a time when technology is an essential requirement for all humans, and the evidence is the increased dependence on technology in almost every aspect of our lives. Today’s world is evolving with the rapidly growing Internet of Things (IoT)-based application [1]. The rise of the IoT has been a glorious phenomenon in recent years. The physical and virtual objects implanted with sensors, software, and other technologies are interlinked together in IoT [2]. It envisages communicating and sharing data with other devices and systems worldwide over the Internet. Further, IoT is like an array of network-enabled devices that exclude traditional computers such as laptops and servers.

To implement IoT, the traditional technology had to undergo some major modifications. For example, to convert an isolated device into a transmitting device, there is a need to increase small computing devices’ memory and processing capacity while dramatically reducing their size [3]. Further, the creation of various lightweight, secure protocols for communication between different IoT devices is equally important. The improvements to the conventional networks to help the operation of the IoT ecosystem have their own set of consequences. However, the unprecedented growth of interconnected devices has crippled the IoT ecosystem. Consequently, there exists enough scope for threats and attacks in IoT-based applications.

The Global Vice President at New Net Technologies (NNT), Dirk Schrader, stated that IoT-based computers have become the crown jewels of cybercriminals. He also said that less than 42% of businesses can detect insecure IoT devices. Hence, for researchers to develop well-grounded solutions to trace and avert these threats, they must first understand the threats and attacks to make the IoT environment safe, secure, and reliable. There are three significant aspects to consider while examining the IoT from a security perspective. To begin with, there are a massive number of smart devices, possibly billions. This suggests that the IoT would be the most complex man-made system ever in terms of the number of entities involved [4]. Second, they are essentially heterogeneous, with respect to the functionality, protocol stacks, radios, operating systems (some objects do not even have one), energy sources, identities, and so on [5]. Third, each smart object is owned by a company or a person, and it is managed by the same or a different company or individual. Millions of businesses and individuals are in control of a subset of the smart objects in their management domains. From the standpoint of protection, privacy, and trust, how this control is technically upheld is a critical issue.

The state-of-the-art survey on various aspects of IoT, including security, privacy, and robustness, has been presented in [6] by Chen et al. The authors focused on specific issues of IoT interface positioning and localization. The development of lightweight block cipher algorithms has been proposed to be used in devices for data encryption and decryption [7]. A desktop review and qualitative analysis have been performed by Gamudani et al. in [8] to compute performance analysis of attacks. Cryptographic approaches have been discussed in [9] as a method of ensuring long-term security approaches. Different layer architectures of IoT and security issues associated with them have been discussed with possible countermeasures using Blockchain (BC) in [10]. The survey on security aspects of IoT has been presented by Alaba et al. in [11], covering the scope of security countermeasures in some other allied paradigms, including Machine-to-Machine (M2M), Cyber-Physical System (CPS), and Wireless Sensor Networks (WSNs). In [12], Abomhara et al. discussed various applications of IoT and the security threats related to them, including vulnerabilities, intruders, and some other attacks. The threats concerning security and privacy in IoT architecture have been presented without counter measuring techniques by Kozlov et al. in [13].

2. IOT Vulnerability

Vulnerabilities are the defects in a framework's design or usefulness that permits the attacker to execute orders, access unapproved information, and launch distributed denial-of-service (DDoS) attack [14]. Attackers can utilize IoT gadgets with existing issues to infiltrate the networks. DNS rebinding attacks, which allow for the processing and ex-filtration of data from internal networks to new side-channel attacks, such as infrared laser inducted attacks against smart devices in homes and workplaces, are among the risks. In IoT systems, vulnerabilities can be found in several places [15].

Hardware and software systems are two central components of IoT frameworks, vulnerable to design flaws. Regardless of whether bugs are identified due to compatibility and interoperability of the equipment or efforts to remedy them, hardware flaws are very difficult to detect and even more difficult to repair. Computer bugs may exist in operating systems, programming software, and control software. Human elements and programming complexity are two factors that contribute to software configuration defects. Human flaws are normally the source of technical vulnerabilities [16]. Miscommunication between the developer and clients, lack of resources, skills, and experience, and a failure to manage and monitor the system can result from a poor understanding of the specifications introducing vulnerabilities in the IoT framework. Thus, vulnerability poses indispensable threats and attacks in the IoT environment. What follows next is the taxonomy of threats and attacks in IoT.

3. Taxonomy of Threats and Attacks in IoT

A threat is an activity that exploits a system's security flaws and has a negative effect on it. Humans and the environment are the two main sources of security threats [17][18]. As an example, seismic tremors, typhoons, floods, and fires are all natural hazards that can cause serious damage to computer systems. Few shields can be used to protect against traumatic events since these naturally occurring events cannot be prevented. Backup and contingency planning, for example, are the best ways to protect stable infrastructures from common threats. Human threats are those that humans create, such as malicious threats that are either internal (someone has allowed access) or external (individuals or organizations operating outside the network) in nature and seek to damage or disrupt a system. Following are the different types of human threats:

- Unstructured threats: These are made up mainly of novice people who use the readily available hacking software.
- Structured threats: People aware of system vulnerabilities and can comprehend, build, and exploit code and scripts are known as structured risks.
- Advanced Persistent Threats (APT): A coordinated assault is an example of advanced persistent threats. APT is a sophisticated network attack that seeks to steal data from high-value information in industries such as manufacturing, banking, and national defense [19].

A taxonomy of threats posing a big concern from a security perspective in the IoT environment is shown in **Figure 1**.

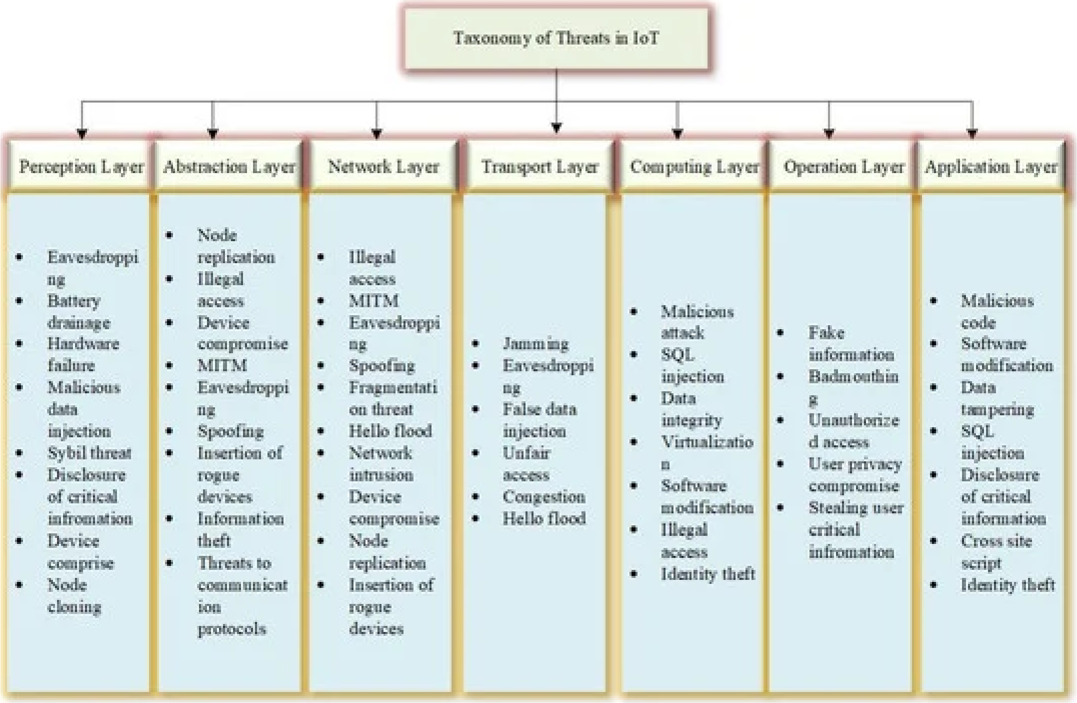
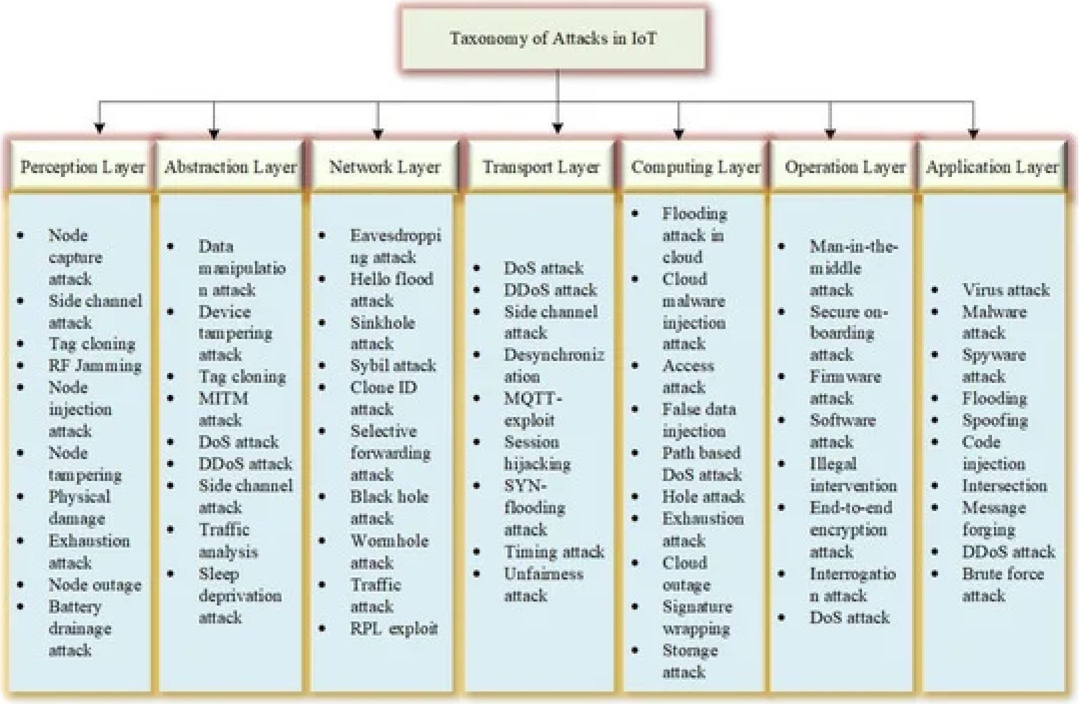


Figure 1. Taxonomy of threats in IoT.

Compared to the threat that can be intentional or unintentional, the attack is always intentional and malicious to cause damage. Several security attacks persist in the IoT framework, which can be analyzed with respect to the proposed IoT reference model. A taxonomy of attacks in IoT has been presented in **Figure 2**. These threats and attacks pose severe challenges to the IoT environment from a security perspective. The security concern due to various threats and attacks are categorically described in the following subsections.



Taxonomy of Attacks in IoT

Perception Layer	Abstraction Layer	Network Layer	Transport Layer	Computing Layer	Operation Layer	Application Layer
• Node capture attack • Side channel attack • Tag cloning • RF Jamming • Node injection attack • Node tampering • Physical damage • Exhaustion attack • Node outage • Battery drainage attack	• Data manipulation attack • Device tampering attack • Tag cloning • MITM attack • DoS attack • DDoS attack • Side channel attack • Traffic analysis • Sleep deprivation attack	• Eavesdropping attack • Hello flood attack • Sinkhole attack • Sybil attack • Clone ID attack • Selective forwarding attack • Black hole attack • Wormhole attack • Traffic attack • RPL exploit	• DoS attack • DDoS attack • Side channel attack • Desynchronization • MQTT-exploit • Session hijacking • SYN-flooding attack • Timing attack • Unfairness attack	• Flooding attack in cloud • Cloud malware injection attack • Access attack • False data injection • Path based DoS attack • Hole attack • Exhaustion attack • Cloud outage • Signature wrapping • Storage attack	• Man-in-the-middle attack • Secure on-boarding attack • Firmware attack • Software attack • Illegal intervention • End-to-end encryption attack • Interrogation attack • DoS attack	• Virus attack • Malware attack • Spyware attack • Flooding • Spoofing • Code injection • Intersection • Message forging • DDoS attack • Brute force attack

Figure 2. Taxonomy of attacks in IoT.

4. Security Goals and Roadmap in IoT

There are certain security objectives that IoT must essentially meet to provide undisputed services. For smooth functioning, IoT applications require secure connections with proper authentication mechanisms and data confidentiality. To ensure information security, one needs to implement the CIA triad—data Confidentiality, Integrity, and Availability. Threats and violations in any of these areas can result in substantial damage to the system, compromise its integrity, and disrupt its activity. To be efficient in implementing effective IoT security, the following primary security objectives must be considered. These security objectives can be achieved with effective methodologies for detection, prevention, and mitigation of threats and attacks pertaining to the IoT ecosystem, described in the next section.

- Confidentiality: Confidentiality is an important security feature in the Internet of Things, but it is not always required, for example, in cases where data are exchanged with the public. In the vast majority of situations and cases, sensitive data must not be disclosed or read by unauthorized persons [20]. Sensitive information about patient data, company information, and possibly military information, as well as security accreditations, should all be kept private from unauthorized users. Confidentiality should be granted such that the information gathered or distributed is safe and only accessible to approved users. Data collected by a computer or a sensor should not be sent to other devices unless they are properly encrypted. To prevent malicious actors from accessing the collected data, only encrypted messages should be sent to neighboring devices. A data encryption system transforms each bit of data into ciphertext, followed by a two-step verification process in which two devices/components permit access only if the authentication test is passed by both the devices, and a biometric verification in which the user is uniquely identifiable and biometric authentication in which the person can be identified by his or her fingerprints.

- Integrity: Integrity should be offered to ensure data validity. Data integrity is critical since data recipients must be able to verify whether data obtained from other devices are authentic. In most cases, integrity is a necessary security property for IoT users to receive reliable services [21]. Different IoT systems have different levels of trustworthiness. As an example, because of data sensitivities, a patient observation framework would have high trustworthiness testing against arbitrary mistakes. It is integrated into the network to protect cybercrimes data in the communication process so that data manipulation cannot be carried out without the danger detected by the device. Two error detection methods are used to ensure data integrity in the inspection and cyclic redundancy search. For continuous data sync for backup purposes, a version control system is used.

- Authentication and authorization: Authenticity is related to credibility, and it means that each system in the network should be able to recognize and authenticate other devices. Since the IoT is made up of so many devices, it is critical to be able to recognize them; otherwise, malicious devices might use spoofing to target IoT networks. Due to the design of IoT settings, the possible communication between the device and device (M2M) is exacerbated by the problem of authentication in IoT connectivity. Different authentication criteria in different systems require different solutions. Some solutions, such as bank card or bank device authentication, require a high level of reliability. However, others will need to be foreign, such as e-Passport, while others will need to be local. Only approved entities (any authenticated entity) can conduct such network operations using the authorization property [22].

- Availability: The primary aim of every IoT protection system is to make data available to users promptly. The consumer should be able to obtain data from the resources right away, not only in usual circumstances but also in emergencies. Firewalls are installed in the network to protect against attacks on services such as denial-of-service attacks, which prevent data from reaching the end-user [23].

- Accountability: Accountability provides redundancy and responsibility for some activities, tasks, and the preparation of the execution of network security policies while designing security strategies to be used in a safe network [24]. Accountability cannot prevent attacks on its own, but it does help ensure that other security measures are functioning properly. Integrity and confidentiality, for example, can be rendered worthless if they are not subjected to transparency. Often, in a disapproved event, an entity’s behavior can also be traced through an accountability system, which can help determine the inside story of what occurred and who was ultimately responsible.

5. Conclusions

The introduction of smart computing devices using IoT has made day-to-day lives more convenient. Data analytics, automation, and smart devices have all benefited from the introduction of IoT into human life. Nevertheless, the unprecedented growth in IoT has also been crippled with many vulnerabilities and challenges. Further, the IoT's heterogeneous design expands the attack surface and adds new challenges to an already vulnerable IoT network. The successful compromise of the system's security may have fatal consequences for users. The overall security of the device must be considered to ensure that critical vulnerabilities are mitigated. Policies and protocols must be enforced as much as possible to deter threats and attacks. In this paper, we have presented a most comprehensive survey on IoT from the perspective of security threats and attacks. Further, modern threats and attacks on the emerging IoT infrastructure, security flaws, and countermeasures are discussed in this paper. In addition, a roadmap of using ubiquitous technologies, viz., BC, FC, EC, and ML, for enhancing security in IoT are comprehensively discussed in this paper.

However, due to IoT devices' heterogeneous existence and limitations, any resolution would be ineffective and obsolete. Consequently, due to the evolving nature of technology, it is estimated that more countermeasures and vulnerabilities will be revealed in the near future. As future work, the authors are working on ML and IoT integration to enhance IoT-based applications' security under dynamically varying conditions.

References

1. Jha, A.V.; Appasani, B.; Ghazali, A.N. Performance Evaluation of Network Layer Routing Protocols on Wireless Sensor Networks. In Proceedings of the 2019 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 17–19 July 2019; pp. 1862–1865.
2. Tiwary, A.; Mahato, M.; Chidar, A.; Chandrol, M.K.; Shrivastava, M.; Tripathi, M. Internet of Things (IoT): Research, architectures and applications. Int. J. Future Revolut. Comput. Sci. Commun. Eng. 2018, 4, 23–27.
3. Ryan, P.J.; Watson, R.B. Research Challenges for the Internet of Things: What Role Can OR Play? Systems 2017, 5, 24.
4. Jha, A.V.; Appasani, B.; Ghazali, A.N.; Pattanayak, P.; Gurjar, D.S.; Kabalci, E.; Mohanta, D.K. Smart grid cyber-physical systems: Communication technologies, standards and challenges. Wirel. Netw. 2021, 27, 2595–2613.
5. Jha, A.V.; Mishra, S.K.; Appasani, B.; Ghazali, A.N. Communication Networks for Metropolitan E-Health Applications. IEEE Potentials 2021, 40, 34–42.
6. Chen, L.; Thombre, S.; Järvinen, K.; Lohan, E.S.; Alén-Savikko, A.; Leppäkoski, H.; Bhuiyan, M.Z.H.; Bu-Pasha, S.; Ferrara, G.N.; Honkala, S.; et al. Robustness, security and privacy in location-based services for future IoT: A survey. IEEE Access 2017, 5, 8956–8977.

7. Shin, H.; Lee, H.K.; Cha, H.Y.; Heo, S.W.; Kim, H. IoT security issues and light weight block cipher. In Proceedings of the International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Okinawa, Japan, 11–13 February 2019; pp. 381–384.
8. Gamundani, A.M. An impact review on internet of things attacks. In Proceedings of the International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Windhoek, Namibia, 17–20 May 2015; pp. 114–118.
9. Kumar, N.; Madhuri, J.; Channe Gowda, M. Review on security and privacy concerns in Internet of Things. In Proceedings of the International Conference on IoT and Application (ICIOT), Nagapattinam, India, 19–20 May 2017; pp. 1–5.
10. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 2018, 82, 395–411.
11. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. J. Netw. Comput. Appl. 2017, 88, 10–28.
12. Abomhara, M.; Køien, G.M. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. J. Cyber Secur. Mobil. 2015, 4, 65–88.
13. Kozlov, D.; Veijalainen, J.; Ali, Y. Security and privacy threats in IoT architectures. BODYNETS 2012, 256–262.
14. Pipkin, D.L. Halting the Hacker: A Practical Guide to Computer Security, 2nd ed.; Prentice Hall Professional: Hoboken, NJ, USA, 2003.
15. Bertino, E.; Martino, L.D.; Paci, F.; Squicciarini, A.C. Web services threats, vulnerabilities, and countermeasures. In Security for Web Services and Service-Oriented Architectures; Springer: Heidelberg, Germany, 2019; pp. 25–44.
16. Kizza, J.M. Guide to Computer Network Security, 1st ed.; Springer: Heidelberg, Germany, 2009; pp. 387–411.
17. Dahbur, K.; Mohammad, B.; Tarakji, A.B. A survey of risks, threats and vulnerabilities in cloud computing. In Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications, New York, NY, USA, 18–20 April 2011; pp. 1–6.
18. Rainer, R.K.; Cegielski, C.G. Ethics, privacy, and information security. In Introduction to Information Systems: Supporting and Transforming Business; John Wiley & Sons: Hoboken, NJ, USA, 2010; Volume 3, pp. 70–121.
19. Tankard, C. Advanced persistent threats and how to monitor and deter them. Netw. Secur. 2011, 2011, 16–19.
20. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. Comput. Netw. 2015, 76, 146–164.

21. Cherian, M.; Chatterjee, M. Survey of security threats in iot and emerging countermeasures. In Proceedings of the International Symposium on Security in Computing and Communication, Bangalore, India, 19–22 September 2018; pp. 591–604.
22. Sepulveda, J.; Willgerodt, F.; Pehl, M. SEPUFSoC: Using PUFs for memory integrity and authentication in multi-processors system-on-chip. In Proceedings of the GLSVLSI ‘18: Proceedings of the 2018 on Great Lakes Symposium on VLSI, Chicago, IL, USA, 23–25 May 2018; pp. 39–44.
23. Bîrleanu, F.G.; Bizon, N. Reconfigurable computing in hardware security–a brief review and application. J. Electr. Eng. Electron. Control Comput. Sci. 2016, 2, 1–12.
24. Katsikogiannis, G.; Kallergis, D.; Garofalaki, Z.; Mitropoulos, S.; Douligeris, C. A policy-aware Service Oriented Architecture for secure machine-to-machine communications. Ad Hoc Netw. 2018, 80, 70–80.

Retrieved from https://encyclopedia.pub/entry/history/show/33104