IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Role Of Artifcial Intelligence In The Internet Of Things (Iot) Cybersecurity

Mrs Seema Bhushan Dhalpe

Abstract

In recent years, the use of the Internet of Things (IoT) has increased exponentially, and cybersecurity concerns have

Increased along with it. On the cutting edge of cybersecurity is Artifcial Intelligence (AI), which is used for the development of complex algorithms to protect networks and systems, including IoT systems. However, cyber-attackers have fgured out how to exploit AI and have even begun to use adversarial AI in order to carry out cybersecurity attacks. This review paper compiles information from several other surveys and research papers regarding IoT, AI, and attacks with and against AI and explores the relationship between these three topics with the purpose of comprehensively presenting and summarizing relevant literature in these felds

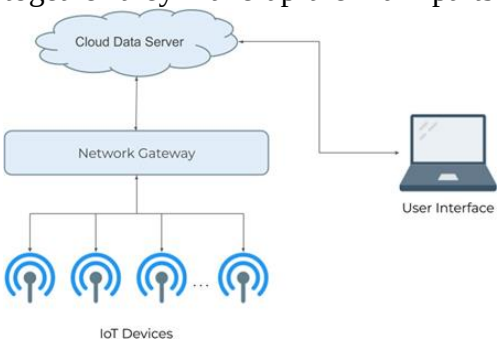
Keywords Artifcial Intelligence · Internet of Things (IoT) · Cybersecurity

I. INTRODUCTION

Since around 2008, when the Internet of Things (IoT) was born [1], its growth has been booming, and now IoT is a part of daily life and has a place in many homes and businesses. IoT is hard to defne as it has been evolving and changing since its conception, but it can be best understood as a network of digital and analog machines and computing devices provided with unique identifers (UIDs) that have the ability to exchange data without human intervention [2]. In most cases, this manifests as a human interfacing with a central hub device or application, often a mobile app, that then goes on to send data and instructions to one or multiple fringe IoT devices [3]. The fringe devices are able to complete functions if required and send data back to the hub device or application, which the human can then view. The IoT concept has given the world a higher level of accessibility, integrity, availability, scalability, confdentiality, and interoperability in terms of device connectivity [4]. However, IoTs are vulnerable to cyberattacks due to a combination of their multiple attack surfaces and their newness and thus lack of security standardizations and requirements [5]. There are a large variety of cyberattacks that attackers can leverage against IoTs, depending on what aspect of the system they are targeting and what they hope to gain from the attack. As such, there is a large volume of research into cybersecurity surrounding IoT. This includes Artifcial Intelligence (AI) approaches to protecting IoT systems from attackers, usually in terms of detecting unusual behavior that may indicate an attack is occurring [6]. However, in the case of IoT, cyber-attackers always have the upper hand as they only need to fnd one vulnerability while cybersecurity experts must protect multiple targets. This has led to increased use of AI

2 Methods of attacking IoT devices Due to the lax security in many IoT devices, cyberattackers have found many ways to attack IoT devices from many different attack surfaces. Attack surfaces can vary from the IoT device itself, both its hardware and software, the network on which the IoT device is connected to, and the application with which the device interfaces; these are the three most commonly used attack surfaces as

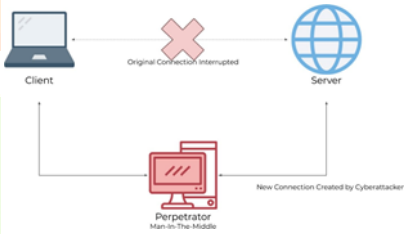
together they make up the main parts of an IoT s



2.1 Initial reconnaissance Before IoT attackers even attempt cyberattacks on an IoT device, they will often study the device to identify vulnerabilities. This is often done by buying a copy of the IoT device they are targeting from the market. They then reverse engineer the device to create a test attack to see what outputs can be obtained and what avenues exist to attack the device. Examples of this include opening up the device and analyzing the internal hardware—such as the fash memory—in order to learn about the software, and tampering with the microcontroller to identify sensitive information or cause unintended behavior [16]. In order to counter reverse engineering, it is important for IoT devices to have hardware-based security. The application processor, which consists of sensors, actuators, power supply, and connectivity, should be placed in a tamper-resistant environment [16]. Device authentication can also be done with hardware-based security, such that the device can prove to the server it is connected to that it is not fake.

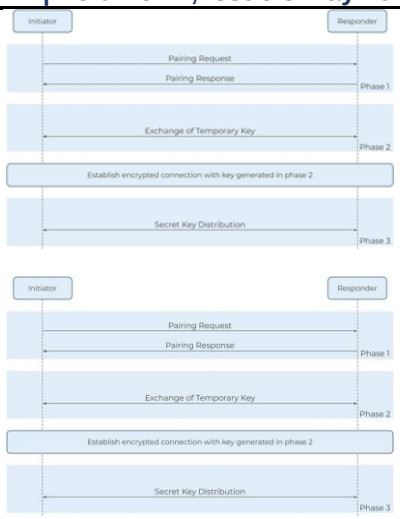
2.2 Physical attacks An often low-tech type category of attacks includes physical attacks, in which the hardware of the target device is used to the beneft of the attacker in some way. There are several diferent types of physical attacks. These include attacks such as outage attacks, where the network that the devices are connected to are shut of to disrupt their functions; physical damage, where devices or their components are damaged to prevent proper functionality; malicious code injection, an example of which includes an attacker plugging a USB containing a virus into the target device; and object jamming, in which signal jammers are used to block or manipulate the signals put out by the devices [17]. Permanent denial of service (PDoS) attacks, which are discussed later in this paper, can be carried out as a physical attack; if an IoT device is connected to a high voltage power source, for example, its power system may become overloaded and would then require replacement [18].

2.3 Man-in-the-Middle One of the most popular attacks on IoTs is Man-in-the-Middle (MITM) attack. With regards to computers in general, an MITM attack intercepts communication between two nodes and allows the attacker to take the role of a proxy. Attackers can perform MITM attacks between many diferent connections such as a computer and a router, two cell phones, and, most commonly, a server and a client. Figure 2 shows a basic example of an MITM attack between a client and a server. In regards to IoT, the attacker usually performs MITM attacks between an IoT device and the application with which it interfaces. IoT devices, in particular, tend to be more vulnerable to MITM attacks as they lack the standard implementations to fght the attacks. There are two common modes of MITM attacks: cloud polling and direct connection. In cloud polling, the smart home device is in constant communication with the cloud, usually to look for frmware updates. Attackers can redirect network trafc using Address Resolution Protocol (ARP) poisoning or by altering Domain Name System (DNS) settings or intercept HTTPS trafc by using self-signed certifcates or tools such as (Secure Sockets Layer) SSL strip



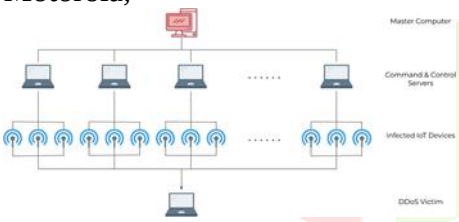
[19]. Many IoT devices do not verify the authenticity or the trust level of certifcates, making the self-signed certifcate method particularly efective. In the case of direct connections, devices communicate with a hub or application in the same network. By doing this, mobile apps can locate new devices by probing every IP address on the local network for a specifc port. An attacker can do the same thing to discover devices on the network [19]. An example of an MITM IoT attack is that of a smart refrigerator that could display the user's Google calendar. It seems like a harmless feature, but attackers found that the system did not validate SSL certifcates, which allowed them to perform an MITM attack and steal the user's Google credentials [19]. 2.3.1 Bluetooth Man-in-the-Middle A common form of MITM attack leveraged against IoT devices is via Bluetooth connection. Many IoT devices run Bluetooth Low Energy (BLE), which is designed with IoT devices in mind to be smaller, cheaper, and more power-efcient [20]. However, BLE is

vulnerable to MITM attacks. BLE uses AES-CCM encryption; AES encryption is considered secure, but the way that the encryption keys are exchanged is often insecure. The level of security relies on the pairing method used to exchange temporary keys between the devices. BLE specifcally uses three-phase pairing processes: frst, the initiating device sends a pairing request, and the devices exchange pairing capabilities over an insecure channel; second, the devices exchange temporary keys and verify that they are using the same temporary key, which is then used to generate a short-term key (some newer devices use a long-term key exchanged using Elliptic Curve Dife-Hellman public-key cryptography, which is signifcantly more secure than the standard BLE protocol); third, the created key is exchanged over a secure connection and can be used to encrypt data [20]. Figure 3 represents this three-phase pairing process. The temporary key is determined according to the pairing method, which is determined on the OS level of the device. There are three common pairing methods popular with IoT devices. One, called Just Works, always sets the temporary key to 0, which is obviously very insecure. However, it remains one of if not the most popular pairing methods used with BLE devices [20]. The second, Passkey, uses six-digit number combinations, which the user must manually enter into a device, which is fairly secure, though there are methods of bypassing this [20]. Finally, the Out-of-Band pairing method exchanges temporary keys using methods such as Near Field Communication. The security level of this method is determined by the security capabilities of the exchange method. If the exchange channel is protected from MITM attacks, the BLE connection can also be considered protected. Unfortunately, the Out-of-Band method is not yet common in IoT devices [20]. Another important feature of BLE devices is the Generic Attribute Profle (GATT), which is used to communicate between devices using a standardized data schema. The GATT describes devices' roles, general behaviors, and other metadata. Any BLE-supported app within the range of an IoT device can read its GATT schema, which provides the app with necessary information [20]. In order for attackers to perform MITM attacks in BLE networks, the attacker must use two connected BLE devices himself: one device acting as the IoT device to connect to the target mobile app, and a fake mobile app to connect to the target IoT device. Some other tools for BLE MITM attacks exist, such as GATTacker,



2.3.2 False data injection attacks Once an attacker has access to some or all of the devices on an IoT network via an MITM attack, one example of an attack they could carry out next is a False Data Injection (FDI) attack. FDI attacks are when an attacker alters measurements from IoT sensors by a small amount so as to avoid suspicion and then outputs the faulty data [21]. FDI attacks can be perpetrated in a number of ways, but in practice doing so via MITM attacks is the most practical. FDI attacks are often leveraged against sensors that send data to an algorithm that attempts to make predictions based on the data it has received or otherwise uses data to make conclusions. These algorithms, sometimes referred to as predictive maintenance systems, are commonly used in monitoring the state of a mechanical machine and predicting when it will need to be maintained or tuned [21]. These predictive maintenance algorithms and similar would also be a staple feature of smart cities, FDI attacks against which could be disastrous. An example of an FDI attack on a predictive maintenance system is sensors on an airplane engine that predict when the engine will need critical maintenance. When attackers are able to access even a small portion of the sensors, they are able to create a small amount of noise that goes undetected by faulty data detection mechanisms but is just enough to skew the algorithm's predictions [21]. In testing, it would even be enough to delay critical maintenance to the system, potentially causing catastrophic failure while in use, which could cause a costly unplanned delay or loss of life. 2.4 Botnets Another kind of common attack on IoT devices is recruiting many devices to create botnets and launch Distributed Denial of Service (DDoS) attacks. A denial of service (DoS) attack is characterized by an orchestrated efort to prevent legitimate use of a service; a DDoS attack uses attacks from multiple entities to achieve this goal. DDoS attacks aim to overwhelm the infrastructure of the target service and disrupt normal data fow.

DDoS attacks generally go through a few phases: recruitment, in which the attacker scans for vulnerable machines to be used in the DDoS attack against the target; exploitation and infection, in which the vulnerable machines are exploited, and malicious code is injected; communication, in which the attacker assesses the infected machines, sees which are online and decides when to schedule attacks or upgrade the machines; and attack, in which the attacker commands the infected machines to send malicious packets to the target [22]. One of the most popular ways to gain infected machines and conduct DDoS attacks is through IoT devices due to their high availability and generally poor security and maintenance. Figure 4 shows a common command structure, in which the attacker's master computer sends commands to one or more infected command and control centers, who each control a series of zombie devices that can then attack the target. One of the most famous malware, the Mirai worm, has been used to perpetrate some of the largest DDoS attacks ever known and is designed to infect and control IoT devices such as DVRs, CCTV cameras, and home routers. The infected devices become part of a large-scale botnet and can perpetrate several types of DDoS attacks. Mirai was built to handle multiple diferent CPU architectures that are popular to use in IoT devices, such as x86, ARM, Sparc, PowerPC, Motorola,



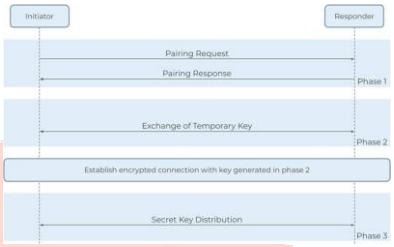
2.5 Denial of service attacks IoT devices may often carry out DoS attacks, but they themselves are susceptible to them as well. IoT devices are particularly susceptible to permanent denial of service (PDoS) attacks that render a device or system completely inoperable. This can be done by overloading the battery or power systems or, more popularly, frmware attacks. In a frmware attack, the attacker may use vulnerabilities to replace a device's basic software (usually its operating system) with a corrupted or defective version of the software, rendering it useless [18]. This process, when done legitimately, is known as fashing, and its illegitimate counterpart is known as "phlashing". When a device is phlashed, the owner of the device has no choice but to fash the device with a clean copy of the OS and any content that might've been put on the device. In a particularly powerful attack, the corrupted software could overwork the hardware of the device such that recovery is impossible without replacing parts of the device [18]. The attacks to the device's power system, though less popular, are possibly even more devastating. One example of this type of attack is a USB device with malware loaded on it that, when plugged into a computer, overuses the device's power to the point that the hardware of the device is rendered completely ruined and needs to be replaced [18]. One example of PDoS malware is known as BrickerBot. BrickerBot uses brute force dictionary attacks to gain access to IoT devices and, once logged in to the device, runs a series of commands that result in permanent damage to the device. These commands include misconfguring the device's storage and kernel parameters, hindering internet connection, sabotaging device performance, and wiping all fles on the device [24]. This attack is devastating enough that it often requires reinstallation of hardware or complete replacement of the device. If the hardware survives the attack, the software certainly didn't and would need refashing, which would lose everything that might have been on it. Interestingly enough, BrickerBot was designed to target the same devices the Mirai botnet targets and would employ as bots, and uses the same or a similar dictionary to make its brute force attacks. As it turns out, BrickerBot was actually intended to render useless those devices that Mirai would have been able to recruit in an efort to fght back against the botnet [24]. Due to the structure of IoT systems, there are multiple attack surfaces, but the most popular way of attacking IoT systems is through their connections as these tend to be the weakest links. In the future, it is advisable that IoT developers ensure that their products have strong protections against such attacks, and the introduction of IoT security standards would prevent users from unknowingly purchasing products that are insecure. Alternatively, keeping the network that the IoT system resides on secure will help prevent many popular attacks, and keeping the system largely separated from other critical systems or having backup measures will help mitigate the damage done should an attack be carried out.

II. CONLUSION

6 Conclusion Due to the nature of IoT systems to have many attack surfaces, there exists a variety of attacks against these systems, and more are being discovered as IoT grows in popularity. It is necessary to protect systems against these attacks as efectively as possible. As the number and speed of attacks grow, experts are turning to AI as a means of protecting these systems intelligently

and in real-time. Of course, attackers fnd ways to thwart these AI and may even use AI to attack systems. This paper explores popular techniques to attempt to disrupt or compromise IoT and explains at a surface level how these attacks are carried out. Where applicable, examples are also provided in order to clarify these explanations. Next, several producers and the companies supplying services in the field align themselves with environmental policies and agree to the proposals of non-governmental organizations regarding methods of diminishing the negative effects of hardware and software. This paper discusses the contribution of cloud computing to environmental protection according to the studies on this topic undertaken so far.

2.3.1 Bluetooth Man-in-the-Middle A common form of MITM attack leveraged against IoT devices is via Bluetooth connection. Many IoT devices run Bluetooth Low Energy (BLE), which is designed with IoT devices in mind to be smaller, cheaper, and more power-efcient [20]. However, BLE is vulnerable to MITM attacks. BLE uses AES-CCM encryption; AES encryption is considered secure, but the way that the encryption keys are exchanged is often insecure. The level of security relies on the pairing method used to exchange temporary keys between the devices. BLE specifcally uses three-phase pairing processes: frst, the initiating device sends a pairing request, and the devices exchange pairing capabilities over an insecure channel; second, the devices exchange temporary keys and verify that they are using the same temporary key, which is then used to generate a short-term key (some newer devices use a long-term key exchanged using Elliptic Curve Dife-Hellman public-key cryptography, which is signifcantly more secure than the standard BLE protocol); third, the created key is exchanged over a secure connection and can be used to encrypt data [20]. Figure 3 represents this three-phase pairing process. The temporary key is determined according to the pairing method, which is determined on the OS level of the device. There are three common pairing methods popular with IoT devices. One, called Just Works, always sets the temporary key to 0, which is obviously very insecure. However, it remains one of if not the most popular pairing methods used with BLE devices [20]. The second, Passkey, uses six-digit number combinations, which the user must manually enter into a device, which is fairly secure, though there are methods of bypassing this [20]. Finally, the Out-of-Band pairing method exchanges temporary keys using methods such as Near Field Communication. The security level of this method is determined by the security capabilities of the exchange method. If the exchange channel is protected from MITM attacks, the BLE connection can also be considered protected. Unfortunately, the Out-of-Band method is not yet common in IoT devices [20]. Another important feature of BLE devices is the Generic Attribute Profle (GATT), which is used to communicate between devices using a standardized data schema. The GATT describes devices' roles, general behaviors, and other metadata. Any BLE-supported app within the range of an IoT device can read its GATT schema, which provides the app with necessary information [20]. In order for attackers to perform MITM attacks in BLE networks, the attacker must use two connected BLE devices himself: one device acting as the IoT device to connect to the target mobile app, and a fake mobile app to connect to the target IoT device. Some other tools for BLE MITM attacks exist, such as GATTacker,



V . References

References 1. Evans D. The Internet of Things: how the next evolution of the internet is changing everything. Cisco Internet Business Solutions Group: Cisco; 2011. 2. Rouse M. What is IoT (Internet of Things) and how does it work? IoT Agenda, TechTarget. http://www.internetofthingsagenda.techtarget.com/ defnition/Internet-of-Things-IoT. Accessed 11 Feb 2020. 3. Linthicum D. App nirvana: when the internet of things meets the API economy. https://techbeacon.com/app-dev-testing/app-nirvana-wheninternet-things-meets-api-economy. Accessed 15 Nov 2019. 4. Lu Y, Xu LD. Internet of Things (IoT) cybersecurity research: a review of current research topics. IEEE Internet Things J. 2019;6(2):2103–15. 5. Vorakulpipat C, Rattanalerdnusorn E, Thaenkaew P, Hai HD. Recent challenges, trends, and concerns related to IoT security: aan evolutionary study. In: 2018 20th international conference on advanced communication technology (ICACT), Chuncheon-si Gangwon-do, Korea (South); 2018. p. 405–10. 6. Lakhani A. The role of artifcial intelligence in IoT and OT security.

https://www.csoonline.com/article/3317836/the-role-of-artificial-intelligen ce-in-iot-and-ot-security.html. Accessed 11 Feb 2020. 7. Pendse A. Transforming cybersecurity with AI and ML: view. https://ciso.economictimes.indiatimes.com /news/transforming-cybersecuritywith-ai-and-ml/67899197. Accessed 12 Feb 2020. 8. Meneghello F, Calore M, Zucchetto D, Polese M, Zanella A. IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet Things J. 2019;6(5):8182–201. 9. Roopak M, Yun Tian G, Chambers J. Models deep learning, for cyber security in IoT networks. In: IEEE 9th annual computing and communication workshop and conference (CCWC), Las Vegas, NV, USA. 2019;2019:0452–7. 10. Cañedo J, Skjellum A. Using machine learning to secure IoT systems. In: 2016 14th annual conference on privacy, security and trust (PST), Auckland; 2016. p. 219–22, https://doi.org/10.1109/PST.2016.7906930 . 11. Farivar F, Haghighi MS, Jolfaei A, Alazab M. Artifcial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT. IEEE Trans Ind Inf. 2020;16(4):2716–25. https://doi.org/10.1109/TII.2019.2956474. 12. Wang S, Qiao Z. Robust pervasive detection for adversarial samples of artifcial intelligence in IoT environments. IEEE Access. 2019;7:88693–704. https://doi.org/10.1109/ACCESS.2019.291 9695. 13. Radanliev P, De Roure D, Van Kleek M, Santos O, Ani U. Artifcial intelligence in cyber physical systems. AI & society. 2020; p. 1–14. 14. Radanliev P, De Roure D, Page K, Nurse JR, Mantilla Montalvo R, Santos O, Maddox LT, Burnap P. Cyber risk at the edge: current and future trends on cyber risk analytics and artifcial intelligence in the industrial internet of things and industry 4.0 supply chains. Cybersecurity. 2020;3:1–21. 15. Radanliev P, De Roure DC, Nurse JR, Montalvo RM, Cannady S, Santos O, Burnap P, Maple C. Future developments in standardisation of cyber risk in the Internet of Things (IoT). SN Appl Sci. 2020;2(2):169. 16. Woo S. The right security for IoT: physical attacks and how to counter them. In: Minj VP, editor. Proft From IoT. http://www.iot.electronicsforu .com/headlines/the-right-security-for-iot-physical-attacks-and-how-to-counter-them/. Accessed 13 June 2019. 17. Akram H, Dimitri K, Mohammed M. A comprehensive iot attacks survey based on a building-blocked reference mode. Int J Adv Comput Sci Appl. 2018. https://doi.org/10.14569/IJACSA.2018.09 0349. 18. Herberger C. DDoS fre & forget: PDoS—a permanent denial of service. Radware Blog, Radware Ltd. http://www.blog.radware.com/secur ity/2015/10/ddos-fre-forget-pdos-a-permanent-denial-of-service/. Accessed 12 Sept 2016. 19. Cekerevac Z, Dvorak Z, Prigoda L, Čekerevac P. Internet of things and the man-in-the-middle attacks–security and economic risks. Mest J. 2017;5:15–25. https://doi.org/10.12709/mest.05.05.02.03. 20. Melamed T. An active man-in-the-middle attack on bluetooth smart devices. WIT Press, International Journal of Safety and Security Engineering. http://www.witpress.com/elibrary/sse-volumes/8/2/2120. Accessed 1 Feb 2018. 21. Mode G, Calyam P, Hoque K. False data injection attacks in Internet of Things and deep learning enabled predictive analytics; 2019. 22. De Donno M, Dragoni N, Giaretta A, Spognardi A. Analysis of DDoS-capable IoT malwares. In: 2017 federated conference on computer science and information systems (FedCSIS), Prague; 2017. p. 807–16. https://doi.org/10.15439/2017F288. 23. Mirai Botnet DDoS Attack. Corero, Corero. http://www.corero.com/resource-hub/mirai-botnet-ddos-attack/. Accessed 9 Dec 2019. 24. BrickerBot Malware emerges, permanently bricks iot devices. Trend Micro, Trend Micro Incorporated. http://www.trendmicro.com/vinfo/us/ security/news/internet-of-things/brickerbot-malware-permanently-bricks-iot-devices. Accessed 19 Apr 2017. 25. Zeadally S, Adi E, Baig Z, Khan IA. Harnessing artifcial intelligence capabilities to improve cybersecurity. IEEE Access. 2020;8:23817–37. 26. Jurn J, Kim T, Kim H. An automated vulnerability detection and remediation method for software security. Sustainability. 2018;10:1652. https ://doi.org/10.3390/su10051652. 27. Comiter M. Attacking artifcial intelligence. Belfer Center for Science and International Afairs, Belfer Center for Science and International Afairs. http://www.belfercenter.org/sites/default/fl

es/2019-08/AttackingAI/AttackingAI.pdf. Accessed 25 Aug 2019. 28. McMahan B, Daniel R. Federated learning: collaborative machine learning without centralized training data. Google AI Blog, Google. http:// www.ai.googleblog.com/2017/04/federated-learning-collaborative.html. Accessed 6 Apr 2017. 29. Rojek M. Federated learning for IoT. Medium, becoming human: artifcial intelligence magazine. http://www.becominghuman.ai/theres-abetter-way-of-doing-ai-in-The-iot-era-feabbbc1b589. Accessed 16 Apr 2019. Content courtesy of Springer Nature, terms of use apply. Rights reserved. Vol:.(1234567890) Review Discover Internet of Things (2021) 1:7 | https://doi.org/10.1007/s43926-020-00001-4 1 3 30. Porter E. What is a botnet? And how to protect yourself in 2020. SafetyDetectives, Safety Detectives. http://www.safetydetectives.com/blog/what-is-a-botnet-and-how-to-protect-yourself-in/#review-2. Accessed 28 Dec 2019. 31. Hendrickson J. What is the mirai botnet, and how can i protect my devices? How to geek, LifeSavvy media. http://www.howtogeek.com/40803 6/what-is-the-mirai-botnet-and-how-can-i-protect-my-devices/. Accessed 22 Mar 2019. 32. Understanding denial of service attacks. Cybersecurity and infrastructure security agency CISA. http://www.us-cert.cisa.gov/ncas/tips/ST04- 015. Accessed 20 Nov 2019. 33. Moisejevs I. Poisoning attacks on machine learning. Towards data science, medium. http://www.towardsdatascience.com/poisoning-attac ks-on-machine-learning-1f247c254db. Accessed 15 July 2019. 34. Fang M et al. Local model poisoning attacks to Byzantine-Robust federated learning. In: Usenix security symposium. arXiv:1911.11815. Accessed 6 Apr 2020. Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional afliations