JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Role of Artificial Intelligence in the Internet of Things (IoT) With Cyber security

G.R.Thejasree[1],G.Visawas[2] ,D.Narendra[3],Ch.Saipavan[4], Dr G Chenchukrishnaiah[5*]
[Department of ECE, Audisankara college of engineering and technology, Gudur, Andhra Pradesh, India]

Abstract
In recent years, the use of the Internet of Things (IoT) has increased exponentially, and cyber security concerns have increased along with it. On the cutting edge of cyber security is Artificial Intelligence (AI), which is used for the development of complex algorithms to protect networks andsystems, including IoT systems. However, cyber-attackers have figured out how to exploit AI and have even begun to use adversarial AI in order to carry out cyber security attacks. This review papercompiles information from several other surveys and research papers regarding IoT, AI, and attackswith and against AI and explores the relationship between these three topics with the purpose of comprehensively presenting and summarizing relevant literature in these felids.

Introduction
Since around 2008, when the Internet of Things (IoT) was born, 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 define as it has been evolving and changing since its conception, but it can be best understood as a networkof digital and analogy machines and computing devices provided with unique identifiers (UIDs) thathave the ability to exchange data without human intervention. In most cases, this manifests as a human interfacing with a central hub device or application, often a mobile app, that then goes on tosend data and instructions to one or multiple fringe IoT devices. The fringe devices are able to complete functions if required and send data back to the hub device or application, which the humancan then view.

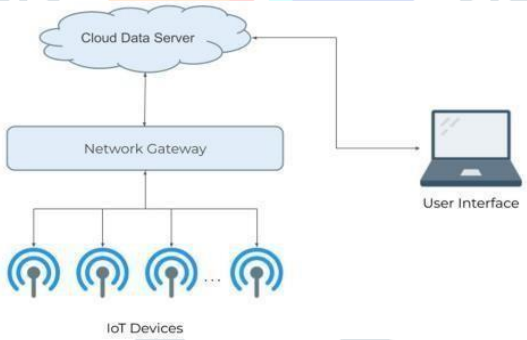
The IoT concept has given the world a higher level of accessibility, integrity, availability, scalability, confidentiality, and interoperability in terms of device connectivity. However, IoTs are vulnerable to cyber-attacks due to a combination of their multiple attack surfaces and their newness and thus lack of security standardizations and requirements. There are a large variety of cyber-attacks 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 cyber security surrounding IoT.

This includes Artificial Intelligence (AI) approaches to protecting IoT systems from attackers, usually in terms of detectingunusual behavior that may indicate an attack is occurring. However, inthe case of IoT, cyber-attackers always have the upper hand as they only need to find one vulnerability while cyber security experts must protect multiple targets. This has led to increased use of AI by cyber- attackers as well, in order to thwart the complicated algorithms that detect anomalous activity and pass by unnoticed. AI has received much attention with the growth of IoT technologies. With this growth, AI technologies, such as decision trees, linear regression, machine learning, support vector machines, and neural networks, have been used in IoT cyber security applications to able to identify threats and potential attacks.
Authors in provide a comprehensive review of the security risks related to IoT application and possible counteractions as well as compare IoT technologies in terms of integrity, anonymity, confidentiality, privacy, access control, authentication, authorization, resilience, and self- organization. The authors propose deep learning models using CICIDS2017 datasets for DDoS attack detection for the cyber security in IoT (Internet of Things), which provide high accuracy, i.e.,97.16%. In, the authors evaluate the Artificial Neural Networks (ANN) in a gateway device to able

to detect anomalies in the data sent from the edge devices. The results show that the proposed approach can improve the security of IoT systems. The authors in propose an AI- based control approach for detection and estimation as well as compensation of cyber- attacks in industrial IoT systems. In, the authors provide a robust pervasive detection for IoT Environments and develop a variety of adversarial attacks and defense mechanisms against them as well as validate their approach through datasets including MNIST, CIFAR-10, and SVHN. In, the authors analyze the recent evolution of AI decision- making in cyber physical systems and find that such evolution is virtually autonomous due to the increasing integration of IoT devices in cyber physical systems, and the value of AI decision-making due to its speed and efficiency in handling large loads of data is likely going to make this evolution inevitable. The authors of discuss new approaches to risk analytics using AI and machine learning, particularly in IoT networks present in industry settings. Finally, discusses methods of capturing and assessing cyber security risks to IoT devices for the purpose of standardizing such practices so that risk in IoT systems may be more efficiently identifiedand protected against. This review paper covers a variety of topics regarding cyber security, the Internet of Things (IoT), Artificial Intelligence (AI), and how they all relate to each other in three survey-style sections and provides a comprehensive review of cyber-attacks against IoT devices aswell as provides recommended AI-based methods of protecting against these attacks. The ultimate goal of this paper is to create a resource for others who are researching these prevalent topics by presenting summaries of and making connections between relevant works covering different aspectsof these subjects.

Methods of attacking IoT devices

Due to the lax security in many IoT devices, cyber attackers 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 surfacesas together they make up the main parts of an IoT system. Figure 1 illustrates a basic breakdown ofa common IoT system; most of the attacks discussed in this paper occur at the network gateway and/or cloud data server connections, as these connections are generally where IoT security is mostlacking.



Initial reconnaissance

Before IoT attackers even attempt cyber-attacks 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 thedevice and analyzing the internal hardware—such as the flash memory—in order to learn about thesoftware, and tampering with the microcontroller to identify sensitive information or cause unintended behavior. In order to counter reverse engineering, it is important for IoT devices to havehardware-based security. The application processor, which consists of sensors, actuators, power supply, and connectivity, should be placed in a tamper- resistant environment. Device authenticationcan 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.

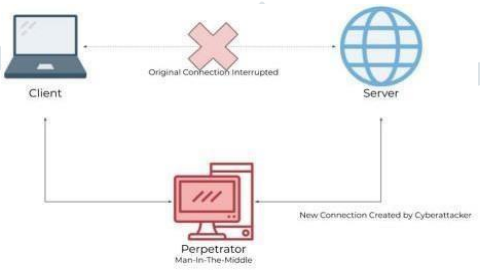
Physical attacks

An often low-tech type category of attacks includes physical attacks, in which the hardware of the target device is used to the benefit of the attacker in some way. There are several different types ofphysical attacks. These include attacks such as outage attacks, where the network that the devices are connected to are shut off 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.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.

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 theattacker to take the role of a proxy. Attackers can perform MITM attacks between many different 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 theapplication with which it interfaces. IoT devices, in particular, tend to be more vulnerable to MITMattacks as they lack the standard implementation to fight the attacks. There are two common modes of MITM attacks: cloud polling and direct connection. In cloud polling, the smart homedevice is in constant communication with the cloud, usually to look for firmware updates. Attackerscan redirect network traffic using Address Resolution Protocol (ARP) poisoning or by
altering Domain Name System (DNS) settings or intercept HTTPS traffic by using self-signed



certificates or tools such as (Secure Sockets Layer) SSL strip.

Many IoT devices do not verify the authenticity or the trust level of certificates, making the self- signed certificate method particularly effective. In the case of direct connections, devices communicate with a hub or application in the same network. By doing this, mobile apps can locatenew devices by probing every IP address on the local network for a specific port. An attacker can do the same thing to discover devices on the network. An example of an MITM IoT attack is that ofa 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 certificates, which allowed them to performan MITM attack and steal the user's Google credentials .

Bluetooth Man-in-the-Middle

A common form of MITM attack leveraged against IoT devices is via Bluetooth connection. ManyIoT devices run Bluetooth Low Energy (BLE), which is designed with IoT devices in mind to be smaller, cheaper, and more power-efficient. 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 specifically uses three-phase pairing processes:first, the initiating device sends a pairing request, and the devices exchange pairing capabilities overan insecure channel; second, the devices exchange temporary keys and verify that they are using thesame temporary key, which is then used to generate a short-term key (some newer devices use a long-term key exchanged using Elliptic Curve Dief- Hellman public-key cryptography, which is significantly more secure than the standard BLE protocol); third, the created key is exchanged overa secure connection and can be used to encrypt data. Figure 3 represents this three-phase pairing process. The temporary key is determined according to the pairing method, which is determined onthe 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. 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. Finally, the Out-of-Band pairing method exchanges temporary keys using methods such as Near Field Communication. The securitylevel 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. Another important feature of BLE devices is the Generic Attribute profile (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. In order forattackers 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 fakemobile app to connect to the target IoT device. Some other tools for BLE MITM attacks exist, suchas GATTacker.

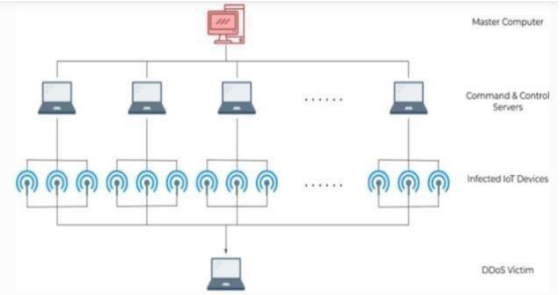
A Node.js package that scans and copies BLE signals and then runs a cloned version of the IoT device, and BtleJuice, which allows MITM attacks on Bluetooth Smart devices which have improvedsecurity over BLE.

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 examples of an attack they could carry out next is a False Data Injection(FDI) attack. FDI attacksare when an attacker alters measurements from IoT sensors by a small amount so as to avoid suspicion and then outputs the faulty dat.FDI attacks can be perpetrated in a number of ways, but inpractice 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. These predictive maintenanceAlgorithms and similar would also be a staple feature of smart cities, FDI attacks against which would be disastrous. An example of an FDI attack on a predictive maintenance system is sensors onan 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'spredictions. 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.

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 effort 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 infrastructureof the target service and disrupt normal data flow. DDoS attacks generally go through a few phases:recruitment, in which the attacker scans vulnerable machines to be used in the DDoS attack againstthe target; exploitation and infection, in which the vulnerable machines are exploited, and maliciouscode 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. 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 different CPUarchitectures that are popular to use in IoT devices, such as x86, ARM, Sparc, PowerPC, Motorola,etc., in order to capture as many devices as possible. In order to be covert, the virus is quite small and actually does not reside in the device's hard disk. It stays in memory, which means that once the device is rebooted, the virus is lost. However, devices that have been infected once are susceptible to reinfection due to having already been discovered as being vulnerable, and reinfectioncan take as little as a few minutes. Today, many well-known IoT-targeting botnet viruses are derivedfrom Mirai's source code , including Okiru, Satori, and Reaper.

AI to attack IoT

Not all AI is used for the purposes of cybersecurity; cybercriminals have begun using malicious AIto aid attacks, often to thwart the intrusion detection algorithms in the case of IoT, or attacking beneficial AI in such a way that the AI works against its own system.

Automation of vulnerability detection

Machine learning can be used to discover vulnerabilities in a system. While this can be useful for those trying to secure a system to intelligently search for vulnerabilities that need to be patched, attackers also use this technology to locate and exploit vulnerabilities in their target system. As technology soars in usage, especially technologies with low-security standards such as IoT devices,the number of vulnerabilities that attackers are able to exploit has soared as well, including zero-dayvulnerabilities. In order to identify vulnerabilities quickly, attackers often use AI to discover vulnerabilities and exploit them much more quickly than developers can fix them. Developers are able to use these detection tools as well, but it should be noted that developers are at a disadvantagewhen it comes to securing a system or device; they must find and correct every single vulnerability that could potentially exist, while attackers need only find one, making automatic detection a valuable tool for attackers.

Fuzzing

Fuzzing, at its core, is a testing method that generates random inputs (i.e., numbers, chars, metadata,binary, and especially "known-to-be-dangerous" values such as zero, negative or very large numbers, SQL requests, special characters) that causes the target software to crash. It can be dividedinto dumb fuzzing and smart fuzzing. Dumb fuzzing simply generates defects by randomly changingthe input variables; this is very fast as changing the input variable is simple, but it is not very good at finding defects as code coverage is narrow [26]. Smart fuzzing, on the other hand, generates inputvalues suitable for the target software based on the software's format and error generation. This software analysis is a big advantage for smart fuzzing as it allows the fuzzing algorithm to know where errors can occur; however, developing an efficient smart fuzzing algorithm takes expert knowledge and tuning.

Symbolic execution

Symbolic execution is a technique similar to fuzzing that searches for vulnerabilities by setting inputvariables to a symbol instead of a real value. This technique is often split into offline and online symbolic execution. Offline symbolic execution chooses only one path to explore at a time to createnew input variables by resolving the path predicate. This means that each time one wishes to explorea new path, the algorithm must be run from the beginning, which is a disadvantage due to the largeamount of overhead due to code re-execution. Online symbolic execution replicates states and generates path predicates at every branch statement. This method does not incur much overhead, butit does require a large amount of storage to store all the status information and simultaneous processing of all the states it creates, leading to significant resource consumption.

Input attacks

When an attacker alters the input of an AI system in such a way that causes the AI to malfunctionor give an incorrect output, it is known as an input attack. Input attacks are carried out by adding an attack pattern to the input, which can be anything from putting tape on a physical stop sign to confuseself-driving cars to adding small amounts of noise to an image that is imperceptible to the human eye but will confuse an AI. Notably, the actual algorithm and security of the AI does not need to becompromised in order to carry out an input attack— only the input that the attacker wants to compromise the output of must be altered. In the case of tape on a stop sign, the attacker may not need to use technology at all. However, more sophisticated attacks are completely hidden from thehuman eye, wherein the attacker may alter a tiny part of the image in a very precise manner that is designed to misdirect the algorithm. That being said, input attacks are often categorized based on where they rest on two axes: perceivability and format.

The perceivability of an input attack is the measure of how noticeable the attack is to the human eye, while the format is the measure of how digital versus physical the attack is. On one end of the perceivability axis is perceivable attacks. Altering targets, such as by deforming, removing part of,or changing its colors, and adding to the target, such as affixing physical tape or adding digital marks, are types of perceivable attacks. While perceivable attacks are perceivable by humans, humans may not notice slight changes like tape on a stop sign or consider them important. A humandriver still sees a stop sign with tape or scratches as a stop sign, even though a self-driving car maynot. This lends itself to the effectiveness of perceivable attacks, allowing them to, in many cases, hide in plain sight. Conversely, imperceivable attacks are invisible to the human eye. This can include things such as “digital dust,” which is a small amount of noise added to the entire image thatis not visible to the human eye but significant enough to an AI to change its output or an imperceptible pattern on a 3D printed object that can be picked up by AI. Imperceivable attacks canalso be made through audio, such as playing audio at ranges outside of the human hearing range thatwould be picked up by a microphone. Imperceivable attacks are generally more of a security risk, as there is almost no chance that a human would notice the attack before the AI algorithm outputs an incorrect response.

The format of an attack is usually either digital or physical, without many attacks that are a combination of both. In many cases of physical attacks, the attack pattern must be more obvious rather than imperceivable as physical objects must be digitized to be processed and, in that process,may lose some finer detail. Some attacks are still difficult to perceive even with the detail loss, however, as with the case of 3D printed objects with a pattern that blends into the structure of the object such that it is imperceptible to humans. Opposite of physical attacks are digital attacks, whichattack digital inputs such as images, videos, audio recordings, and files. As these inputs are alreadydigitized, there is no process wherein detail is lost, and as such attackers can make very exact attacks, allowing them to be more imperceptible to the human eye than physical attacks. Digital attacks are not necessarily imperceptible. However—photoshopping glasses with a strange pattern over a celebrity, for example, may cause the AI to identify the image as a different person, but still a personnonetheless. An example of input attacks specific to IoT smart cars and, more broadly, smart cities.As mentioned earlier, simply placing pieces of tape in a specific way on a stop sign is enough for an algorithm to not recognize the stop sign or even classify it as a green light—this is harmful for passengers in the car if the car does not heed the stop sign, and at a larger scale could alter traffic pattern detectors in smart cities. Additionally, noise-based input attacks could cause smart assistantsto malfunction and carry out unintended commands.

Data poisoning/false data injection

Data poisoning attacks and input attacks are very similar, but while the goal of input attacks is simply to alter the output of the affected input, the goal of data poisoning is to alter inputs over a long enough period of time that the AI that analyzes data has shifted and is inherently flawed; because of this, data poisoning is usually carried out while the AI is still being trained before it is actually deployed. In many cases, the AI learns to fail on specific inputs that the attacker chooses; for example, if a military uses AI to detect aircraft, the enemy military may poison the AI so that itdoes not recognize certain types of aircraft like drones. Data poisoning can also be used on AIs thatare constantly learning and analyzing data in order to make and adjust predictions, such as in predictive maintenance systems. There are three main methods attackers can use to poison an AI.

Summary of attacks and their defenses

The various attacks discussed in this paper are listed in Table 1, and are paired with one or more ways of protecting an IoT system from the attack. While comprehensively protecting an IoT systemcan be a challenging task due to the number of attack surfaces present, many of the methods listed will defend against many types of

attacks; for example, as many of the attacks listed are carried outby first conducting MITM attacks, protecting the network on which an IoT system resides will protect the system from many common attacks.

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 effectively as possible. As the number and speed of attacksgrow, experts are turning to AI as a means of protecting these systems intelligently and in real-time.Of course, attackers find 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 levelhow these attacks are carried out. Where applicable, examples are also provided in order to clarify these explanations. Next, several AI algorithms are introduced, and their applications in cybersecurity are investigated. In many cases, these models are not yet common in commercial applications but rather are still undergoing research and development or are still difficult to implement and thus rare. Nonetheless, the models discussed are promising and may become common attack detection systems within just a couple of years. Methods of attacking AI and using AI to attack are also discussed, with the frame of IoT systems. The growth of IoT systems will see these types of attacks become more and more of a threat, especially as massive networks such as smart cities begin experimentation; both as massive networks are harder to protect with a multitudeof attack surfaces, and as daily life and safety revolve around AI which needs to be more or less failure-proof. This is followed by a chart reiterating the threats covered in this paper, paired with common or recommended methods of protecting against each attack. Having covered all these topics, this paper aims to provide a useful tool with which researchers and cybersecurity professionals may study IoT in the context of cybersecurity and AI in order to secure IoT systems. Additionally, it also aims to emphasize the implications of up and coming technology and the impacts that each of means diverting the technology from its original have been taken advantage offor criminal purposes or have had weaknesses exploited as an example of this, which will help readers understand current risks and help cultivate an understanding such that these weaknesses are accounted for in the future in order to prevent cyberattacks.

REFERENCE

[1] Rouse M. What is IoT (Internet of Things) andhow does it work? IoT AgendaTechTarget. http://www.internetofthingsagen da.techtarget.com/definition/Internet-of- Things-IoT. Accessed 11Feb 2020.

[2] Linthicum D. App nirvana: when the internet ofthings meets the APIeconomy. Evans D. The Internet of Things: how the next https://techbeacon.com/app-dev- testing/appnirvana-when- internet-things- meets-api-economy. Accessed 15 Nov 2019.

[3] 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.

[4] 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.

[5] Lakhani A. The role of artificial intelligence inIoT and OTsecurity. https://www.csoonline.com/article/3317836/therole-of-artificial-intelligence-in- iot-and- otsecurity.html. Accessed 11 Feb2020.

[6] Pendse A. Transforming cybersecurity with AIand ML: view. https://ciso.economictimes.indiatimes.com/news/transforming-cybersecurity-with-aiand-ml/67899197. Accessed 12 Feb 2020.