A survey on Classification of Cyber-attacks on IoT and IIoT devices

Yash Shah
Computer Science and Engineering Department
University of Nevada, Reno
Reno, Nevada, 89557
Email: yashs@nevada.unr.edu

Shamik Sengupta
Computer Science and Engineering Department
University of Nevada, Reno
Reno, Nevada, 89557
Email: ssengupta@unr.edu

***Abstract*—Internet of Things (IoT) devices have gained popularity in recent years. With the increased usage of IoT devices, users have become more prone to Cyber-attacks. Threats against IoT devices must be analyzed thoroughly to develop protection mechanisms against them. An attacker's purpose behind launching an attack is to find a weak link within a network and once discovered, the devices connected to the network become the primary target for the attackers. Industrial Internet of Things (IIoT) emerged due to the popularity of IoT devices and they are used to interconnect machines, sensors, and actuators at large manufacturing plants. By incorporating IIoT at their facilities companies have benefited by reducing operational costs and increasing productivity. However, as IIoT relies on utilizing the Internet to operate it is vulnerable to Cyber-attacks if security is not taken into consideration. After seeing the advantages of IIoT, a new version of smart industries has been introduced called Industry 4.0. Industry 4.0 combines cloud and fog computing, cyber-physical systems (CPS), and data analytics to automate the manufacturing process. This paper surveys the different classifications of attacks that an attacker can launch against these devices and mentions methods of mitigating such attacks[1].**

***Index Terms*—IoT, IIoT, Industry 4.0, Cyber-attacks, Cyber-security, Cloud Computing**

I. Introduction

The number of IoT devices used is expected to reach 75 billion by 2025 [1], increasing apprehensions around the security of such devices. IoT devices can communicate with each other via the Internet, therefore forming a network and allowing interconnection between such devices for easier control. Examples of such devices are smart lights, thermostats, speakers, ACs, refrigerators, TVs, sensors, etc. [2], [3]. With every new IoT device introduced and used, the risk of Cyber-attacks on such devices and the networks they form increases. In recent years, securing these systems has become a major concern, hindering their usage in certain crucial fields such as warfare and surveillance [3]. Despite implementing various methods to secure IoT systems, there will always be new forms of attacks introduced due to differences in security standards amongst manufacturers. Even if IoT devices are secure on their own when connected to an unsecured network they become vulnerable to numerous attacks.

[1]This research is supported by NSF award #1739032.

Before the introduction of the Industrial Internet of Things (IIoT) industries utilized Supervisory Control and Data Acquisition (SCADA) systems to monitor and control production plants and their equipment [4]. With the assistance of SCADA systems, production plants can share data and communicate with a central cite to ensure smooth operations. By incorporating IIoT along with SCADA systems large production plants can achieve the goal of becoming a Smart Industry [4]. IIoT is a form of IoT that is used in Manufacturing Industries. IIoT enables interconnection and intelligence for industrial systems with the assistance of sensors and actuators. These systems are dependent on sensor-driven computing, market analysis, and intelligent machine applications which improve productivity and allow for infrastructure automation [5]. They also allow for prediction of equipment failures that assists with reducing maintenance costs and decreasing the likeliness of a potential breakdown further reducing operational costs. While IIoT allows for higher productivity, if the infrastructure and its components are not secure an attack on the infrastructure can be catastrophic and lead to a massive loss.

As IIoT became popular, the advantages that they offered to manufacture plants pioneered the development of Industry 4.0 as it is called in Europe and Smart Manufacturing as it is called in the USA [6]. Industry 4.0 at a manufacturing plant functions on one basic principle: to combine different manufacturing machines, facilities, and companies to create a manufacturing chain. This value chain can greatly benefit from automation, autonomizing, and optimizing operations [6]. Industry 4.0 benefits from the advancements in IIoT, Internet of Service (IoS), Manufacturing Cyber-Physical Systems (CPS), Cloud and Fog manufacturing, and manufacturing analysis to advance. Similar to IIoT once industries start moving toward this new standard of manufacturing they need to be aware of the various types of attacks and need to execute steps towards blocking them since there is a pressing need to buckle down on this issue.

II. Background

A. IoT

IoT devices can be classified into the following three categories [7]:

1) Wearable devices: Wearable devices can be characterized by three different functionalities, such as e-health, communication, and mobile payment [8]. E-health device's main focus is to track people's movements or actions. They are normally connected to a smartphone via Bluetooth which provides the Internet to such devices. Their main usage is in the medical field aiding with tracking patient's mental and physical health. This assists medical professionals while treating a patient as the patient's information is always accessible from anywhere within the premises of a hospital [7]. With the added feature of assisting with communication and mobile payments, it eliminates users having to carry their phones when attempting to tackle these tasks. Examples of such wearable devices are smartwatches, smart clothes, smart jewelry, etc. [7].

2) Smart home devices: Smart home devices allow their consumers to control their home through an app or voice commands from anywhere. These devices include but are not limited to lights, AC/Heater, locks, curtains, refrigerators, and TVs. To control them, these devices are connected to the home's Internet through which they are made accessible for user control.

3) Machine to Machine (M2M) devices: M2M devices can communicate and execute operations without the need for human interaction. These machines are capable of receiving and executing tasks with precision through the Internet thus eliminating the need to hire a human to watch them 24/7. Fields, where M2M devices play a crucial role are telemedicine, robotics, traffic control, the automotive industry, and fleet control [7]. The architecture of M2M devices is split into three different domains that are interconnected. These interlinked domains are called the M2M domain, network domain, and application domain [9]. The functions of each domain are as follows:

a) M2M Domain: This domain contains an array of devices that are used when establishing M2M communications. Among these devices, a few are equipped with sensors to detect changes, while some contain storage capabilities. The collected information is then forwarded to remote servers for further analysis.

b) Network Domain: This domain contains a variety of network devices, used to access the internet and allow communication between domains. The devices that occupy this domain need minimum response times as the M2M and the application domains rely on constant communication. The different access technology used by this domain includes, but is not limited to, Ethernet, xDSL, WiMax, 3G, and LTE [9].

c) Application Domain: This domain consists of the remote servers to which the information is transferred and stored. The information is then made available to authorized users via an application. These applications allow remote data analysis, remote control, and remote sensing.

B. IIoT

For an IIoT to operate properly it must integrate Information Technology (IT) and Operational Technology (OT). In an IIoT architecture, the first three layers consist of OT and the top two layers consist of IT. To split and protect the OT and IT layers there is a demilitarized zone that prevents direct access from one system to another [4].

TABLE I
IIOT LAYERS AND POSSIBLE ATTACKS [4]

IIoT Layers	Components	Possible Attacks
Layer 1	Sensors, Motors, Actuators, Transmitters, and Embedded Devices	Reverse Engineering, Malware, Eavesdropping, Brute Force attack
Layer 2	Distributed Control Systems, Programmable Logic Control (PLC's), and Gateways	Man-in-the-Middle attack, Sniffing, Brute Force attack, Replay attack
Layer 3	Supervisory Control and Data Acquisition (SCADA) Control, Control Room and Operator Stations and Human Machine Interactions (HMI)	IP spoofing, Data sniffing, Data Manipulation, Malware
Layer 4	Data Centers, Office Applications, Intranet, Mail and Web services	Phishing, SQL Injections, Malware, Domain Name Server (DNS) poisoning, Brute Force attack
Layer 5	Business Applications, Cloud Computing, Data Analytics, Internet and Mobile Devices	Denial-of-Service (DoS) attack, Side channel attack, Malware, Password attack, Man-in-the-middle attack

- Layer 1: This layer comprises of devices that assist with physical processes such as embedded devices, sensors, actuators, transmitters, and motors.
- Layer 2: Distributed Control Systems (DCS), Programmable Logic Control (PLC's) and Gateways reside in this layer which is used to interact with the devices that are part of the first layer.
- Layer 3: Supervisory Control and Data Acquisition (SCADA), Data Acquisition devices, and Human Machine Interface (HMI) are part of this layer which aids with the collection and transfer data using the Internet.
- Layer 4: Services that facilitates business planning such as Office Applications, Intranet, Web, and Mail are deployed in this layer. The data which is collected in the third layer is stored in the data centers which are also part of this layer.
- Layer 5: This layer is used for analyzing and mining the data from the data centers to be used by the company executives. The enterprise applications, cloud computing, data analytics, Internet, and mobile devices utilize this layer to gather the necessary data.
- Demilitarized Zone (DMZ): The demilitarized zone acts as a barrier between the IT and OT networks. Devices exposed to the outer world such as application and web servers are part of the DMZ. This zone also prohibits direct access to the OT and IT networks.

C. Industry 4.0

Industry 4.0 is a combination of various components and systems which are integrated to work together. Such systems

are Cyber Physical Systems (CPS), IoT, Cloud, and cognitive computing [6]. There are six different design fundamentals that form the notion of Industry 4.0. The six principles are as follows [6]:

1) Interoperability: the different CPS, robots, machines, and workers need to have the ability to interconnect and communicate with the assistance of the Internet by using IoT or Internet of Service (IoS).

2) Service Oriented: system need to have the ability to portray the manufacturing process functions as a list of services. Along with the ability to make these services accessible over the IoS to the different systems.

3) Decentralization: the different manufacturing systems need the potential of making time-sensitive decisions on their own and avoid the usage of centralized controls. Even though the usage of cloud or fog computing is a key aid in making decisions they should avoid using them to ensure the decision is made in a timely manner.

4) Real-time Capability: these machines should have the ability to immediately collect and analyze the data allowing them to decide on an optimal course of action. The machines should be able to locate their faults, worker's incorrect handling, and decrease in its quality and reliability.

5) Modularity: the elasticity of adapting to the changes, additions, or removal of requirements, along with the ability to function with a new set of processes.

6) Virtualization: the machines should support the ability to create virtual copies of the processes to better monitor them. These copies can be used for testing future enhancements.

III. Classification of Attacks

A. IoT

1) Wearable devices: Wearable devices operate in close proximity to human beings and have access to the most sensitive personal data. Due to their intrinsic nature, wearables are easily prone to Cyber-attacks [8]. These devices can benefit from the interaction of other smart devices such as smart homes, intelligent vehicles, and smart grids. The usage of such devices boosts the trend of mobility; however, this advantage comes with the price of compromising user privacy. Threats against wearable devices can be categorized as follows: Data Integrity, Authenticity, and Privacy [8].

- Data Integrity

  a) Man in the middle attacks: To perform a man in the middle attack, an attacker secretly place's themselves in between the user and the Internet [7]. Whenever a piece of information is requested from the Internet it travels through multiple routers before reaching its intended destination. By placing themselves in the middle, the attackers can read all of the information which passes through them if the data is not encrypted. However, if the data is encrypted and the attackers obtain the key that's used to encrypt the data, the information can be modified. Another variant of this attack is that the attacker will not change any of the information; however, they will store the information that they discover about its victim. These types of attacks are very difficult to detect as there is no way for the user to verify the integrity of the information.

  b) Malicious code injection: A malicious code injection involves changing lines of original code and replacing it with code that may damage the user's system. The malicious code is injected into the wearable device's application allowing an attacker to exploit the system's vulnerability. An attacker can use this method to gain complete access to the wearable device's system threatening both user's privacy and confidentiality by potentially using the access to steal the user's personal data [10].

- Authenticity

  a) Firmware attack: Every device relies on firmware to interconnect the various hardware that are part of a device; wearable devices are no exception. Manufacturers frequently release firmware updates to improve performance or add additional features. In wearable devices, these updates are generally downloaded via a Bluetooth connection. Most of the firmware files are not encrypted during transmission, allowing attackers to easily sniff and modify the traffic between the device and the server [8]. Once the malicious firmware has been transferred to the intended device the only other piece of information that the attacker needs is the architecture of the device's processor which can be easily located by looking at the device's manual. The attacker uses the flaws which exist in the verification of firmware updates to their advantage and the malicious code runs once the firmware updates are installed.

- Privacy

  a) Mole attack: The motion sensors which are part of a smartwatch could be used to launch a mole attack. The sensors are capable of recognizing key stroke patterns from the hand wearing the watch while typing on a keyboard. This information can be used to regenerate the information that was recently typed and depending on the information, the results could be catastrophic. The leaked information could contain passwords to bank accounts, work accounts, security systems, etc. They are also capable of retrieving information that was typed by the other hand and such information leaks do not require any specialized training by an attacker [8].

  b) Account injection attack: A group of researchers analyzed several smartwatches at DEFCON in 2015 and they found that most of the smartwatches had additional protection enabled when disconnected from a smartphone [8]. They also found that when password and USB debugging was enabled attackers could easily access the data through the USB connection and a command line shell. In this mode, the device does not require any additional information to access the command line shell. So, anyone with the knowledge of the system can easily access any private data such as the user account information [8].

2) Smart Home devices: Smart home systems not only enable the control of home devices via smartphones, but they also allow the exchange of data which is used for decision making to ensure user's needs are met. The exchanging of data takes place in a private network that is formed by the

different sensors and actuators using a variety of communication protocols. The usage of such devices does make life easier; however, it can result in security and confidentiality problems. Threats against these devices can be classified into two categories: internal and external system threats [10].

- Internal System threats
  Threats that originate from the device's inner structure are classified as internal system threats. A few instances of such threats are listed below:
  a) Device Failure: Smart home systems rely on constant communication between devices and if one device malfunctions it affects the ongoing communication and poses a physical security threat. For example, if the security cameras control unit fails it will render all of the cameras useless and will not allow a user access to home monitoring while they are away which can lead to strangers accessing the home.
  b) Power or Internet malfunction: The absence of the internet or power in the smart home system may intervene with the services which are being offered. The user will lose the ability to remotely control their home and the systems which rely on both the internet and power will not work at its peak capacity. In the case of the Internet malfunction, the device will not be able to send real-time updates to the smartphone app thus preventing the user to control their own home in case of an intrusion.
  c) Software failure: Smart home systems depend on software to be controlled and operated upon. Any existence of vulnerabilities in the implementation of the software makes those systems a primary target for attackers.
  d) Confidential Data leakage: Smart home systems and apps are in constant communication by exchanging data. If the method of communication lacks the usage of data encryption or communicates using an unsecured mechanism it increases the potential of data leakage or loss of information, in turn increasing cybersecurity threats in the network.
- External System threats
  As mentioned above, these smart home devices are controlled using a smartphone app that is provided by the manufacturer. If the method of wireless communication is vulnerable then it provides an attacker the opportunity to hack or break the system. These types of threats that stem from an outside source are classified as external system threats. A few instances are listed below:
  a) Denial-of-Service (DoS) or Distributed-Denial-of-Service (DDoS) attacks: A DoS attack is used to temporarily or permanently shut down a system/network, not allowing access to anyone. A DDoS attack is a variant of DoS attacks where multiple device are used to launch an attack. These forms of attack are achieved by spamming the intended target with large amounts of access requests so that they are not be able to handle them [3]. DoS and DDoS attacks target a vulnerability that is found in the Transmission Control Protocol (TCP) [11]. In order to connect to the Internet, devices use the TCP's three-way handshake methodology. These attacks exploit TCP's handshake by directing a high volume of requests to establish a TCP connection with the target server. The aim of the attack is to leave the connections in a half-open stage so that these connections exhaust all of the resources of the server such that it is not able to establish new legitimate connections [11]. There are three different scenarios in which this attack can take place. These three scenarios are Insider attack, Outsider attack, and lastly, Masked Insider attack.
  - Insider attack: An attack is classified as an Insider attack when both the attacker and the device used to launch the attack are part of the target network. An example of such an attack is when an employee is planning on leaving the company and wants to damage the company's reputation. They could launch an Insider DoS attack so that the company servers are rendered useless for other users.
  - Outsider attack: An attack is classified as an Outsider attack when both the attacker and the device used to launch the attack are not part of the target network. An example of such an attack is when a company wants to disrupt a rivals company's services. So, they decide to launch an attack against the rival company's network to redirect their customers into using the services offered by them.
  - Masked Insider attack: An attack is classified as a Masked Insider attack when the attacker is outside the target network; however, they have gained access to a device that is part of the target network. An example of such an attack is very similar to an Outsider attack; however, in this case instead of using their device the attacking company decides to hack into a device owned by the rival company to avoid the risk of getting caught. Nonetheless, they will get similar results to an Outsider attack.

  DoS attacks can also be used to disrupt cloud computing. A Cloud DoS attack is achieved through the same means as a regular DoS attack. The attacker targets a particular service offered by a cloud and spams it with large amounts of TCP access requests. When the cloud computing operating system (OS) detects higher workloads, it will attempt to satisfy the need by providing additional computational power [12]. In terms of cloud computing, additional computational power means creating more instances of that service by generating more virtual machines. Eventually, the hardware of the server will run out of computational power to support the service causing it to malfunction or stop. One form of Cloud DoS involves the attacker using a form of an insider attack that contains a host inside the network; these are referred to as Zombies. This form of attack is also known as a Cloud Zombie attack [4].

b) Eavesdropping: Eavesdropping involves illegally listening to personal conversations in real-time by monitoring emails, phone calls, or video conferences. An attacker can listen in on the conversations when the data is being transferred through unsecured servers, when unwanted ports are left open, or when the device is connected to unsecured

public Wi-Fi networks [13].

c) Password attacks: Passwords are often considered as important keys which are used to unlock personal information. Password attacks are carried out using various methods such as password guessing, password resetting, and password capturing. Password guessing, as the name suggests, involves the attacker inputting commonly used password combinations until they find a match. Password re-usage is also another major problem as once the attacker knows the password they can use it to access multiple accounts [13]. Lastly, attackers use a form of a malware to observe the keys used to enter a password.

d) Zero-Day Exploits: Zero-day exploits are vulnerabilities that exist in the latest version of a software that is exploited by hackers and the software manufacturers have yet to find them [7]. This makes these types of attacks extremely dangerous as there is no way to detect or fix the problem yet. Once they have been detected a patch is released to address them and they are no longer called Zero-day exploits.

e) Session Hijacking: During a Session Hijack attack, attackers form a valid temporary session to be used between the server and the user for malicious purposes [13]. To generate the session, the attacker uses authentic cookies from a user's computer to connect to the server. After the valid connection is established the information which is transferred between the client and the server becomes accessible to the attacker.

3) Machine to Machine (M2M) Devices: Attacks on M2M communications are generally divided into two broad categories: passive and active attacks. An attack is categorized as passive when the intent is to collect information and listen to ongoing communications, whereas the aim of an active attack is to makes changes to the device configuration, or network decisions, or to gain control of the base station. These attacks can be further divided into physical, data, and logical attacks on the M2M and network domains based on their targets [9].

- Physical Attacks

  a) Side Channel Attacks: Performing side channel attacks on M2M machines requires physical access to these machines. Attackers can use the peripheral information of the physical devices to extract confidential information from them. These types of attacks can also help attackers retrieve cryptography algorithms keys from the devices [9]. When an M2M device is hosted through the cloud an attacker creates a malicious virtual machine (VM) and places it closer to the target cloud server to potentially compromise that server [12]. Attackers utilize insufficient logical isolation between different VMs on the server to gather the information required for executing such an attack [14]. There are many types of side-channel attacks that are used to target and exploit the server's hardware however, the most common is the cache side-channel attack. During a cache side-channel attack, an attacker targets the cache memory found in a processor to access and analyze the information stored in it. Once the information has been analyzed it is linked to the malicious VM currently occupying the processor [14].

  b) Node Tampering: An attacker requires physical access to an M2M device and takes full control of it. This form of attack is achieved by physically damaging or replacing a node in the device. By doing so the attacker gains complete access to the data stored in its memory and uses it for malicious purposes.

  c) Software Modification: To initiate this type of attack an attacker modifies the software of the device to perform adversely. The modification in the software can target a node causing it to feed inaccurate information to the device violating the integrity of the data. An attacker can carry out this attack both wirelessly and physically.

  d) Hardware Trojans: Hardware Trojans are parts of a device that is manufactured with the intent of being used as malicious and assists attackers in gaining easy access to monitor the device. These additions take place while the device is assembled which makes them impossible to detect. Devices that are purchased from untrusted sources often contain these faults [9].

- Logical Attacks

  a) IP Spoofing: IP addresses play a major role in ensuring the information is sent and received by the intended systems or users. During an IP Spoofing attack, an attacker tries to mimic the behavior of another device by forging the IP address in the packet header when communicating with the Internet [4]. This can be dangerous in a production plant where a machine receives operating instructions via the Internet. If the attacker forges the IP address of a machine then the machine will not receive any instruction which can lead to hazardous working conditions.

  b) Replay attacks: Replay attacks are used when the attacker intends to delay the transfer of information to machines. During this attack, a packet containing future instructions for a machine is captured and sent after an indefinite amount of time. When a packet is captured by an attacker they also have the ability to change the instructions and deceive the machine into performing incorrect tasks.

  c) Routing protocol attacks: During this attack, the routing decisions become the target for attackers. They listen to all of the communication occurring and can make modifications to affect the routing protocols.

- Data Attacks

  a) Traffic Analysis: In this attack, the attacker is constantly monitoring the traffic flowing through the network. While monitoring they are attempting to identify communication patterns and the users involved. Once they have gathered the required information they attempt to distinguish the difference in the information that is sent from sensors, actuators, and actors.

  b) Integrity Attack: The attacker not only targets data in transmission but the data that is stored in any storage device. The attacker can send incorrect data to replace the accurate data that can potentially endanger people's lives. An example of this could be when an attacker modifies the GPS coordinates of an ambulance's destination causing it to arrive at the wrong location and potentially endangering the

patient's life by not arriving on time.

c) Selective Forwarding: In this form of an attack, the attacker delay or drops some of the received communication packets. There are two instances of this attack: black hole and gray hole attacks [9]. In the case of black hole attacks the malicious nodes drops all of the received packets rather than forwarding them. Whereas in the gray hole attack the malicious nodes randomly forward and drop the packets.

B. IIoT and Industry 4.0

Industrial Internet of Things (IIoT) is an extension of the IoT infrastructure which means that IIoT inherits both the benefits and vulnerabilities associated with it. The architecture for IIoT that was previously discussed in section II mentions two classifications in which the components are organized Information Technology (IT) and Operational Technology (OT). The layers associated with IT are made possible by utilizing the Internet and cloud computing. More specifically Layer 5 of the architecture is most exposed to the public due to the fact that it hosts services used to make business decisions.

Cloud computing has been beneficial in allowing the collected data to be stored remotely and be accessible from everywhere for analysis. However, cloud services introduce additional vulnerabilities which depends on the type of cloud service used. Vulnerabilities associated with the different layers of IIoT and cloud computing is exploited by using the following forms of attack:

1) Malware: During this attack, computer code is used to infect a victim's computer causing them to slow down or shut down completely, allowing attackers to steal valuable information [13]. Due to the simplicity of the code, it can spread quickly and possibly infect entire file systems or networks. The longer this code lives on a user's computer the greater the impact it causes. If the systems located in the fourth layer of the architecture are not properly secured there is a possibility of malware making its way down to the layers of OT and infect the devices that reside in those layers causing them to malfunction. There are three common forms of malware spyware, viruses, and worms [7].

Spyware is used to spy on a victim and it's purpose is to obtain the information that is entered by the victims. A computer virus is a computer program that begins replicating itself when executed and replaces original code with malicious code. Computer worms are similar to computer viruses except worms can survive on their own without needing to feed off of a host and spread at a greater rate.

In cloud computing, an attacker utilizes a form of malware and implements a malicious service or VM. Once the malware has been generated they insert it on the cloud system. Once inserted the attacker needs to trick the cloud into thinking that the malware is valid and redirect users to that instance. Once the VM has been infected any users that log into that machine are affected as well.

2) Authentication attacks: When accessing cloud services a user must enter authentic credentials. However, the authentication process and mechanisms are highly vulnerable and often targeted. Many cloud services still utilize single-factor authentication and a simple username and password requirements. Attackers use this vulnerability to their advantage when trying to disrupt services or steal information from an enterprise taking advantage of cloud computing.

3) Phishing attacks: Phishing is used to trick people into entering their personal information or downloading malicious software that is capable of spreading malware. The most common form of phishing attacks are emails that contain links to fake websites, and/or malicious attachments [15]. To execute the attack an attacker creates a fake email that looks legitimate and sends it to an intended user. An example of this would be an email with the subject line of "Congratulations you have won a lottery" or something along those lines and in the body of the email they ask the user to fill out some personal information to obtain the "lottery" they have just earned. However, the user is not aware that the links in the email lead to a fake website that collects that information and uses it for malicious purposes. A similar method is used by attackers to hide malicious software in email attachments.

4) SQL injection: The attackers use SQL injection to gain administrative access to databases by targeting the vulnerabilities in the victim's network [7]. To perform a SQL injection the attacker inputs SQL commands in web forms causing it to execute fraudulent commands to retrieve personal information. If the database or website is not fully secured then it will run those fraudulent commands without hesitation and provide the attack access to the personal information it requested.

5) DNS Spoofing or Poisoning attacks: DNS stands for Domain Name System which is used to translate domain names into IP addresses. To initiate a DNS Spoofing attack an attacker first needs to gain access to one of the DNS servers and change the IP address of a particular domain or website to redirect the users accessing them [16]. DNS Poisoning occurs when the attacker generates a bogus DNS server response and sends it to a DNS server to corrupt the data that was already cached in the DNS server.

6) Web Application attacks: Such attacks occur on the web applications which are part of the web servers in the DMZs. Attackers utilize different forms of Cyber-attacks to disrupt services that are being offered by these servers. Cyber-attacks can range from Malware that can infect the users visiting those web applications, to DoS attacks causing them to malfunction or shut down temporarily.

7) Reverse Engineering: By reverse engineering the source code of embedded systems, attackers can obtain sensitive information regarding that system. Attackers use this method to find sensitive information left by software engineers such as hard-coded credentials and bugs. Once they retrieve the information, they can use it to orchestrate future attacks on the embedded systems. This information is not only used to plan future attacks, they can use the knowledge gained to insert malicious code into the device [4].

IV. Attacks Mitigation Methods and Open Research Challenges

A. Attacks Mitigation Methods

Cyber-attacks often originate from weak or vulnerable links that exists in networks or security systems employed to manage these devices. Attackers are actively looking to exploit these weaknesses to their benefit. Nowadays, everything that is connected to the internet is prone to Cyber-attacks. The interconnection of IoT/IIoT devices benefits attackers as all they are required to do is find one weak link and they can access data from all of the connected devices [7]. In the previous section attacks which are commonly used against IoT and IIoT devices were discussed. In this section, some of the common methods used to protect the system against Cyber-attacks are discussed.

1) Using stronger passwords: Implementing poor password requirements is the primary reason IoT/IIoT networks are targeted [7]. When creating passwords avoid using commonly uses password and incorporate the mixture of uppercase, symbols, and numbers. When generating password ensure that it is unique password for different accounts. Lastly, change the default passwords that are assigned by manufacturers for the device.

2) Updating software: Outdated software may contain flaws that allow attackers to gain access to personal information. Companies often release software updates when the current version contains security vulnerabilities or bugs that can be exploited by attackers. Always ensure to download updates from trusted sources and if possible enroll the device to automatically install updates from the manufacturer's website.

3) Creation of separate networks: When setting up the environment for IoT/IIoT devices ensure that they are kept separate from the rest of the devices to limit the possibility of an external device causing problems. Keeping these devices in a separate private network also eliminates the possibility of an attacker infecting other devices and spreading the malware in the network. Another benefit of this implementation is that only authorized users are going to have the ability to access and modify data.

4) Applying stronger encryption algorithms for the Internet: Guarding of data heavily relies on the form of encryption that is applied when the data is in transit. Encryption turns regular text into a series of random letters and numbers commonly known as ciphertext so that it is not readable to regular users unless they possess a key to convert the cipher text into regular text. Using encryption such as WPA2 when configuring a Wi-Fi router prevents attackers from reading the data even if they have obtained it. If the networks are encrypted the information that is transmitted is secure not allowing an attacker to benefit from it.

5) Changing default settings: Many times the default settings that are assigned by the device manufacturers benefit the company rather than its users. Manufacturers often add or enable features that are not essential in the operation of the device that aids attackers in launching their attacks. These settings should be checked and changed immediately after the device is purchased and setup.

6) Enabling multi-factor authentication: Multi-factor authentication adds an extra layer of security to the authentication methods by requiring additional information to access the device however this feature is disables by default. [7]. Few types of multi-factor authentication are receiving one time codes via text messages or emails, a mobile app, or security questions. As additional information in required to access the device attackers are unable to proceed. An alert is sent to the user so they are made aware of their compromised account.

7) Generate backups: Every device generates data that is analyzed to improve performance. However, attacks similar to ransomware can prevent users or data analysis applications from accessing that data. Creating an automatic backup schedule can ensure that the operations can be easily resumed. Multiple copies of the backup must be created in case a backup is affected. Along with the creation of backups, one needs to ensure that they are accurate and up-to-date to prevent the loss of critical data.

8) Utilization of virtual private networks: Virtual private networks (VPN) can be used to enhance network security as they route traffic through the VPN's servers rather than using the user's Internet service providers (ISP). The data is encrypted and is transferred to VPN's servers through a reliable and pragmatic tunnel [7]. As traffic is routed through VPN's servers, attackers are unable to locate the origin of the data. Another benefit to VPNs is that the characteristic of the data is unknown and devices can be configured to only accept data from the VPN servers [7]. VPNs can be installed inside a router shielding all of the IoT/IIoT devices connected to the router.

B. Open Research Challenges

The concept of IoT/IIoT is fairly new and is constantly evolving along with the research conducted to protect these devices from Cyber-attacks. Attackers are rapidly adapting to changes and finding more ways to exploit vulnerabilities that exist in these devices. This adaptation presents numerous security topics that require further research, hence the name "Open Research Challenges." A few topics which require further research are listed below:

1) Standardization: IoT/IIoT devices are manufactured by various manufacturers; however, each manufacturer has its own set of standards that collide with one another when finding ways to secure such devices. The current architecture of IoT/IIoT consists of a variety of data models, interfaces, and communication protocols. A thorough and generalized IoT/IIoT framework containing integrated data models, ontology, and data formats with protocols, applications, and services needs to be built to fulfill interoperability and integrity of IoT/IIoT mechanisms, applications, and services [17].

2) Big Data: IoT/IIoT devices generate a variety of Big Data and all of the data needs to be processed and transferred outside the IoT network for further analysis. There have been many advancements in protecting data within the IoT network;

however, there hasn't been a lot of research conducted which attempts to protect data once it leaves the network [17]. This data often involves personal information that could have a significant impact on the user's life. The major issues pertaining to data are confidentiality, privacy, and integrity. Protecting data that is outside of the IoT network has introduced new research issues that need to be addressed to properly secure IoT/IIoT devices.

The data generated not only involves personally identifiable information but it contains logs that are generated by network routers to detect anomalies and identify threats, and vulnerabilities that are often discovered after examining the logs. Due to the high volume of traffic generated by various IoT/IIoT devices and their applications, those logs can grow at an exponential rate. Another factor that plays a huge role in the growth of the logs are the different service and communication protocols that are offered and used by these devices thus making it difficult to identify vulnerabilities.

3) Authentication and Authorization: Authentication and Authorization challenges occur when attempting to ensure the security of IoT/IIoT systems in terms of access control and preservation of privacy and integrity. The purpose of the authorization process is to determine which service, resource, or app the user can access. The problem occurs when weak authenticating passwords or poor password management techniques are implemented on the devices. Another factor to consider when resolving these challenges is the evolution of different threats that are constantly being introduced by hackers.

4) Availability: The accessibility and longevity of IoT/IIoT devices need to be maintained for a smooth experience. Problems with availability arise when devices are disconnected or when they experience a failure. Solutions to these problems demand an approach where physical tampering or Cyber-attacks such as Denial-of-Service attacks can be prevented.

V. Conclusion

IoT/IIoT devices have become an important part of our lives. One cannot imagine getting through a day without interacting with one of these devices. With the introduction of automation in certain aspects of IoT devices, in the foreseeable future, there will be devices that will be able to operate freely without needing a human to control them. This invention has fueled the transition of the industrial sector to Smart Industry/Industry 4.0 where large production plants can generate products by utilizing the process of automation. This process heavily relies on the integrity of the data that is transmitted between each sensor and actuator. Since the emergence of IoT in the industry there has been an increase in the number of numerous Cyber-attacks that require attention before determining ways to improve their security.

In this paper, IoT and IIoT devices security issues and challenges were presented with hopes for it to serve as a guide in establishing a secure network for such devices. This paper aims to recognize the different Cyber-attacks which are related to IoT and IIoT devices. Fully securing IoT and IIoT devices is going to be a long process; however, we must understand the different Cyber-attacks that an IoT/IIoT network faces to develop new protection mechanisms.

References

[1] T. Alam, "A reliable communication framework and its use in internet of things (iot)," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT)*, vol. 3, 05 2018.

[2] A. D. Oza, G. N. Kumar, and M. Khorajiya, "Survey of snaring cyber attacks on iot devices with honeypots and honeynets," in *2018 3rd International Conference for Convergence in Technology (I2CT)*, April 2018, pp. 1–6.

[3] M. Anirudh, S. A. Thileeban, and D. J. Nallathambi, "Use of honeypots for mitigating dos attacks targeted on iot networks," in *2017 International Conference on Computer, Communication and Signal Processing (ICCCSP)*, Jan 2017, pp. 1–4.

[4] A. C. Panchal, V. M. Khadse, and P. N. Mahalle, "Security issues in iiot: A comprehensive survey of attacks on iiot and its countermeasures," in *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, Nov 2018, pp. 124–130.

[5] A. Hassanzadeh, S. Modi, and S. Mulchandani, "Towards effective security control assignment in the industrial internet of things," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Dec 2015, pp. 795–800.

[6] J. Al-Jaroodi, N. Mohamed, and I. Jawhar, "A service-oriented middleware framework for manufacturing industry 4.0," *SIGBED Rev.*, vol. 15, no. 5, p. 29–36, Nov. 2018. [Online]. Available: https://doi.org/10.1145/3292384.3292389

[7] G. A. Abdalrahman and H. Varol, "Defending against cyber-attacks on the internet of things," in *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, June 2019, pp. 1–6.

[8] J. Liu and W. Sun, "Smart attacks against intelligent wearables in people-centric internet of things," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 44–49, December 2016.

[9] A. Imani, A. Keshavarz-Haddad, M. Eslami, and J. Haghighat, "Security challenges and attacks in m2m communications," in *2018 9th International Symposium on Telecommunications (IST)*, Dec 2018, pp. 264–269.

[10] K. Karimi and S. Krit, "Smart home-smartphone systems: Threats, security requirements and open research challenges," in *2019 International Conference of Computer Science and Renewable Energies (ICCSRE)*, July 2019, pp. 1–5.

[11] Q. Chen, H. Chen, Y. Cai, Y. Zhang, and X. Huang, "Denial of service attack on iot system," in *2018 9th International Conference on Information Technology in Medicine and Education (ITME)*, Oct 2018, pp. 755–758.

[12] A. Singh and D. M. Shrivastava, "Overview of attacks on cloud computing," *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 1, no. 4, 2012.

[13] H. Teymourlouei, "Quick reference: Cyber attacks awareness and prevention method for home users," *World Academy of Science, Engineering and Technology International Journal of Computer and Systems Engineering*, vol. 9, no. 3, 2015.

[14] Y. A. Younis, K. Kifayat, Q. Shi, and B. Askwith, "A new prime and probe cache side-channel attack for cloud computing," in *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, Oct 2015, pp. 1718–1724.

[15] P. D. Babu, C. Pavani, and C. E. Naidu, "Cyber security with iot," in *2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, vol. 1, March 2019, pp. 109–113.

[16] A. Dua, V. Tyagi, N. Patel, and B. Mehtre, "Iisr: A secure router for iot networks," in *2019 4th International Conference on Information Systems and Computer Networks (ISCON)*, Nov 2019, pp. 636–643.

[17] Y. Lu and L. D. Xu, "Internet of things (iot) cybersecurity research: A review of current research topics," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103–2115, April 2019.