ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

HEY ALEXA, HOW SECURE IS THE INTERNET?

Husein Hakim
Billabong High International School Santacruz
huseinhakim@gmail.com

Abstract

Internet of Things (IoT) devices are growing more common, and IoT services are becoming more widespread. New emerging technologies are influencing the globe today. As a result, we are constantly surrounded by smart devices. These smart devices make life simpler and more convenient for us. Their success has not gone unnoticed, and threats and attacks against IoT devices and services are also on the rise. Cyber-attacks are nothing new in the IoT world, but as the IoT becomes more deeply ingrained in our lives and communities, it will be vital to step up and take cyber defense seriously. As a result, there is a pressing need to secure IoT, which necessitates a thorough understanding of the dangers and attacks against IoT infrastructure. This study aims to categorize threat types as well as assess and characterize intrusions and assaults that affect IoT devices and services.

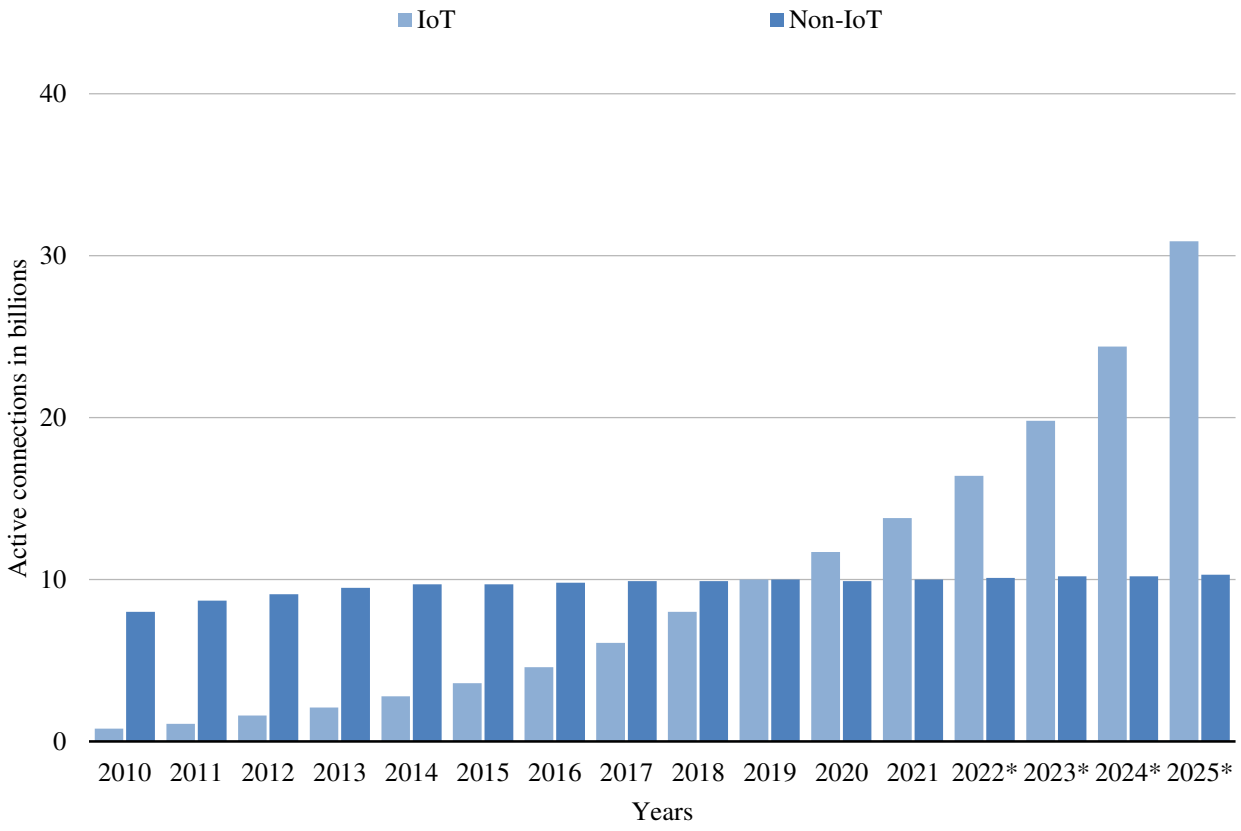
Keywords: *IoT(Internet of Things), Cyber-attack, WSN.*

I. Introduction

IoT refers to a trillion devices that are connected to the internet from all across the world that collect and share data. Due to the advent of super-low-cost computer chips and the ubiquity of wireless networks, something as small as a pill can be converted into something as large as an aircraft into part of the IoT. Connecting and adding sensors to all the various objects adds a digital intelligence level to devices that are otherwise stupid so that they can communicate real-time data without the involvement of a person. The possibilities for personal or professional development are limitless. Insecure connections and data storage are the most common causes of data security concerns in IoT applications. Compromised devices can be exploited to access personal data, which is one of the major challenges for IoT privacy and security.

The unintentional use of passwords, the failure to change passwords, and the lack of device updates have all exacerbated cybersecurity threats and given hostile programmes access to sensitive data in IoT systems. Data breaches and other dangers are more likely as a result of such poor security policies. According to findstacks' reports, 35.82 billion IoT devices will be installed globally by 2021, and 75.44 billion by 2025. As a result of these enormous amount of gadgets, attackers have a surface to attack. The graph below demonstrates how the number of IoT devices have grown as time has passed and technology has progressed.

ISSN 2350-109X
www.indianscholar.co.in
Indian Scholar
An International Multidisciplinary Research e-Journal
MISA MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION



II. Application of IoT

Almost every aspect of our lives is affected by the Internet of Things. Some of the aspects are as follows:

A. Smart Homes

Consider waking up to the scent of coffee while the curtains slowly open behind you. Your sleep sensor has made sure not to disturb you during a session of REM sleep, so you get a

Restful night's sleep. Your voice assistant tells you the weather forecast for the day, suggests

ISSN 2350-109X
www.indianscholar.co.in
Indian Scholar
An International Multidisciplinary Research e-Journal
MISA MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

outfits based on the prediction, and announces your calendar activities, including daily reminders. While you were sleeping, your iRobot softly cleaned. You go to the bathroom, and a smart toilet sensor detects health signs in your pee. Your smart fridge has already submitted an electronic order for milk to an online grocery store since you've ran out of milk for your cereal. This house is the epitome of a smart home. It's all thanks to the Internet of Things!

B. Smart Cars

Self-driving cars have long seemed like something out of a sci-fi movie. Digital technologies have made their way into the automotive sector, thanks to the Internet of Things transforming the transportation industry. The Internet of Things permits human-to-human, machine-to-machine, and human-to-machine connections, all of which will influence how our cars run. Sensors have been added to IoT connected automobiles, allowing them to collect data from their surroundings. These sensors and cameras (such as the reverse camera) give the driver with a continuous stream of diagnostic data on which he or she can act. Some vehicles even feature automatic braking systems that activate when sensors detect something in the vehicle's path.

C. Smart Cities

Cities are becoming digitally networked and hence smarter as a result of the Internet of Things' power. Cities are enhancing the lives of residents by gathering and analysing large quantities of data from IoT devices across many city systems. Data on infrastructure needs, transportation demands, and crime and safety may help smart cities make smarter decisions. According to a research, cities may improve quality of life indices (such as crime, traffic, and pollution) by 10% to 30% by using current smart city apps. In everyday life, IoT devices link to make your house, transit, or city more efficient and pleasurable.

III. IoT communication models

A. The device-to-device communication model

Instead of going via an intermediate application server, two or more devices connect and interact directly with one another. These devices use a variety of networks to connect, including IP networks and the Internet. However, to create direct device-to-device interactions, these devices frequently employ protocols like Bluetooth, Z-Wave, or ZigBee.

B. Device-to-cloud communication model

To exchange data and regulate message flow, the IoT device connects directly to an Internet cloud service, such as an application service provider. This method typically uses existing communication techniques, such as standard wired Ethernet or Wi-Fi connections, to create a link between the device and the IP network, which then connects to the cloud service.

C. Device-to-gateway model/device-to-application-layer gateway (ALG) model

This means that there is application software running on a local gateway device that works as a middleman between the device and the cloud service, providing security and other features like data or protocol translation.

This model may be found in a variety of consumer products. In many situations, a smartphone running an app to connect with a device and pass data to a cloud service serves as the local gateway device. The development of "hub" devices in home automation applications is another

variation of this device-to-gateway paradigm. These are devices that act as a local bridge between IoT devices and cloud services.

D. Back-end data-sharing model

Refers to a communication architecture that allows users to export and analyse smart object data from a cloud service, as well as data from other sources. This design accommodates "the [user's] wish to give third-party access to the uploaded sensor data." This method is a development of the single-device-to-cloud communication paradigm, which might result in data silos if "IoT devices upload data solely to a single application service provider." A federated cloud services strategy, or cloud applications programming interfaces, offers a back-end sharing architecture that allows data gathered from single IoT device data streams to be pooled and analyzed (APIs), to make data from smart devices stored on the cloud interoperable.

IV. IoT security issue

A. Unauthenticated access

Unauthenticated access is one of the most frequent firmware flaws that enable threat actors to get access to an IoT device, making it easier to abuse device data and controls.

B. Weak authentication

When the firmware has a poor authentication mechanism, threat actors can simply obtain access to devices. These techniques can range from single-factor and password-based authentication to cryptographic methods that are vulnerable to brute-force assaults.

C. Hidden backdoors

Hidden backdoors are a popular hacker target when it comes to firmware. Backdoors are deliberate flaws that are implanted in an embedded device to allow anybody with the "secret" authentication information remote access. Although backdoors may be useful for customer assistance, they can have serious repercussions if they are found by hostile actors. Hackers are experts at locating them.

D. Password hashes

Most gadgets' firmware has hard-coded passwords that users can't alter or default passwords that they seldom update. Both of these outcomes provide gadgets that are very simple to exploit. The Mirai botnet, which infected over 2.5 million IoT devices around the world, used default passwords in IoT devices to launch a DDoS assault in 2016, bringing Netflix, Amazon, and The New York Times down with it.

E. Encryption keys

When encryption keys are kept in a format that may be readily hacked, such as variants of the Data Encryption Standard (DES), which was originally established in the 1970s, they can pose a significant threat to IoT security. DES is still in use today, despite the fact that it has been proved to be ineffective. Hackers can use encryption keys to listen in on conversations, get access to the device, or even construct rogue devices capable of performing harmful activities.

F. Buffer overflows

When writing firmware, if the programmer employs unsafe string-handling methods, buffer overflows can occur. Attackers spend a lot of time looking at the code inside a device's software, attempting to find out how to create unpredictable application behaviour or crashes, which can

ISSN 2350-109X
www.indianscholar.co.in
Indian Scholar
An International Multidisciplinary Research e-Journal
MISA MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

lead to a security breach. Buffer overflows can be used to gain remote access to devices and to launch denial-of-service and code-injection attacks.

G. Open source code

The quick creation of complex IoT solutions is made possible by open source platforms and frameworks. However, because IoT devices commonly employ third-party, open source components with unknown or undocumented origins, firmware is usually left unsecured, making it an attractive target for hackers. Although upgrading to the newest version of an open source platform would usually solve the problem, many devices are introduced with known flaws.

H. Debugging services

Developers gain internal system knowledge of a device via debugging information in beta versions of IoT devices. Unfortunately, debugging systems are frequently kept in production devices, allowing hackers to get access to the same inside information.

V. IoT attacks

A. Physical attacks

An attacker gets physical access to a physical asset in the infrastructure system in order to damage, disable, steal, or utilize it in an unfavorable way.

B. Sinkhole attacks

Sinkhole attacks occur when a hacked node attempts to attract network traffic by announcing a bogus routing change. One of the consequences of the sinkhole attack is that it may be used to launch additional attacks such as selective forwarding, acknowledgment spoofing, and routing information drops or changes.

C. Eavesdropping

An eavesdropping assault, also known as a sniffing or spying assault, is when a computer, smartphone, or other connected device steals information while it is sent across a network. The attack uses unprotected network communications to get access to data as it is delivered or received by the user.

D. Reconnaissance attacks

An unauthorized user's attempt to identify and map network system devices, services accessible on those systems, and the vulnerabilities of those systems is known as reconnaissance. It's also known as data collecting, and it usually happens before a real access or Denial of Service (DoS) assault. The malicious intruder will usually start by pinging the target network to see which IP addresses are live and responding. As a result, the intruder may be able to learn what services or ports are active on the live IP addresses. The intruder uses the active IP address information to query the application ports to identify the programme kind and version, as well as the type and version of the operating system.

E. Denial-of-service (DoS)

A denial-of-service (DoS) attack is a type of cyber-attack that prevents legitimate users from accessing computer systems, networks, services, or other information technology (IT) resources. In these sorts of assaults, the attackers often flood web servers, systems, or networks with traffic, overloading the victim's resources and making it difficult or impossible for others to use them.

F. Node Replication

The security of wsn is thought to be jeopardized by replication. On this technique, an attacker attempts to capture sensor nodes by obtaining the credentials of real sensor nodes. Once

captured, the attacker creates a clone or replica of the real node in the same network in order to make it appear that the injected clone is identical to the real node (Game & Raut, 2014). Replicas are difficult to spot since they seem to be legitimate network nodes. It's possible that an attacker will target numerous sensor nodes by capturing the entire cluster or cluster head and creating a clone or copy of the whole cluster.

G. Tag Swapping

Conclusion

The Internet of Things (IoT) has developed as a key technology. The data provided by sensors or RFID tags may include sensitive information that must be kept secure from unwanted access. IoT communication between two nodes is insecure, and IoT device physical security should not be jeopardised. IoT must integrate services like encryption, end-to-end environments, and access control for real-time and critical infrastructure security to accomplish secure communication. Staying one step ahead of the adversary in cybercrime is difficult. We may expect better security for smart devices in the future, as well as higher privacy standards for IoT connectivity, allowing users to automate activities more easily with this technology.

References

1. Mohammed, Husamuddin& Qayyum, Mohammed. (2017). Internet of Things :A Study on Security and Privacy Threats. 10.1109/Anti-Cybercrime.2017.7905270.
2. Mohamed Abomhara and Geir M. Køien. 2015. 'Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks'. Vol(4). Issue 1. Page: 65-88.
3. Jack Steward. The Ultimate List of Internet of Things Statistics for 2021' https://findstack.com/internet-of-things-statistics/
4. 'Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025'https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/
5. https://www.strate.education/gallery/news/iot-daily life#:~:text=Some%20real%2Dworld%20examples%20of,day%20will%20be%20unavoidable%20soon'.
6. 'Unsecured IoT: 8 Ways Hackers Exploit Firmware Vulnerabilities'https://www.darkreading.com/risk/unsecured-iot-8-ways-hackers-exploit-firmware-vulnerabilities/a/d-id/1335564#:~:text=Hackers%20actively%20exploit%20weaknesses%20in,credit%20card%20theft%2C%20among%20others'.
7. G. Wyss, P. Sholander, J. Darby, and J. Phelan. 'Identifying and Defeating Blended Cyber-Physical Security Threats'.
8. George W. Kibirige, Camilius Sanga. 'A Survey on Detection of Sinkhole Attack in Wireless Sensor Network'.
9. Jake Frankenfield 'https://www.investopedia.com/terms/e/eavesdropping-attack.asp#:~:text=An%20eavesdropping%20attack%2C%20also%20known,or%20received%20by%20its%20user'.
10. 'https://cdn.ttgtmedia.com/searchNetworking/downloads/PIXFirewallCH01.pdf'
11. Kevin Ferguson, Peter Loshin. Denial-of-service attack. 'https://searchsecurity.techtarget.com/definition/denial-of-service'.
12. Harpreet Kaur. 2018. UWDBCSN Analysis During Node Replication Attack in WSN. 18 Pages.