Cyber Security for the Internet of Things: A Quick Overview

K. Kishore[1], D. Wasiha Tasneem[2], R. Anil Kumar[3]

[1,2,,3]Asst. Professor, Ashoka Women's Engineering College, Kurnool

Article Info
Page Number: 213 - 217
Publication Issue:
Vol 71 No. 1 (2022)

Article History
***Article Received**: 02 February 2022*
***Revised**: 10 March 2022*
***Accepted**: 25 March 2022*
***Publication**: 15 April 2022*

Abstract

IoT has become increasingly popular in recent years. The technology is crucial. As it has gained in popularity, so have worries about its security. Since the IoT relies only on the internet, any hacker with access to the internet can find a vulnerable point in the infrastructure and steal data, possibly with the intention of keeping, erasing, or making public the stolen information. This includes all kinds of private information and data, as well as health records, intellectual property, and corporate databases. Cybersecurity prevents unauthorised access to computer systems, networks, devices, programmes, and data. Protections against cyberattacks on the Internet of Things are discussed in this study.

Index Terms: Internet of Things(IoT), cyber security.

1. Introduction

The pace and scope of technological development and its effects on our daily lives increase exponentially. The reach of the internet now spans the globe. When close by Internet of Things devices transmit data across the network, security is paramount. Industries also make use of IoT. Consequently, it is crucial to evaluate the potential for cyber vulnerabilities and attacks in the IoT[1] ecosystem and to implement the recommended activities to secure the IoT environment.

The data obtained from the Industrial IoT's network of connected physical devices is used in various analyses. Thousands of sensors and other devices are used in the automated processes of the "smart" industries. Since the goal of the Internet of Things (IoT) is to make people's lives easier by linking together various Internet-enabled devices, IoT ecosystems are susceptible to cyberattacks. For home automation and other industrial uses, the rising popularity of IoT devices represents an exciting new prospect. Once limited to merely computers and mobile devices, internet connectivity has spread to things like televisions, air conditioners, and car cams. In operation, there will be more than 25.4 billion connected devices by the year 2030. The Internet of Things in the Industrial Sector is a cutting-edge innovation. Many issues arise with this cutting-edge technology, but cyber security is a major one.

2. IoT Devices

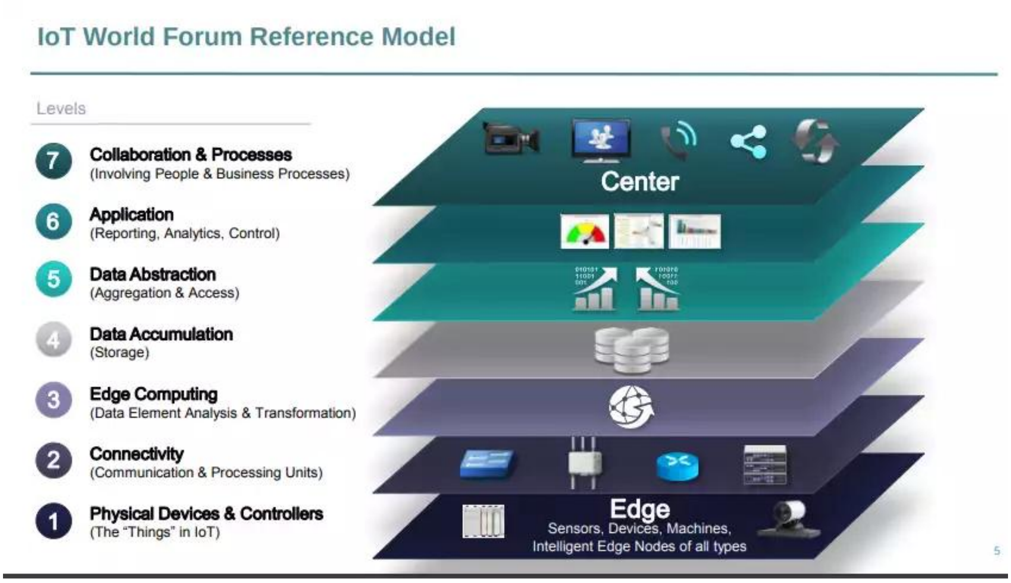
Different types of categories are available for classifying Internet of Things devices. Including sensors, gadgets, and appliances, IoT devices collect and exchange data over the web. Other Internet of Things gadgets can benefit from programmable chips as well. Your car's Internet of Things (IoT) gadget can monitor traffic conditions and send a message to your meeting's other participant[2].

i. **Wearable Devices:** These make up the lion's share of the devices that make up the Internet of Things. These gadgets link to cell phones using Bluetooth and the web in order to monitor the user's activity or behaviour. The data they collect can be used for health monitoring, communication, and activity tracking. Our market is dominated by fitness equipment during the covid-19 epidemic.

ii. **Home Security Devices:** IoT-connected sensors, lights, alarms, and cameras provide security 24 hours a day, seven days a week, and can be controlled through smartphone.

iii. **M2M (Machine to Machine) Devices:** These machines can transmit information and carry out routine tasks with little to no human intervention. The Internet allows these gadgets to receive instructions and carry them out, eliminating the need for constant human oversight. These gadgets are also used Applications for M2M devices include those requiring remote control or monitoring, such as those in the automotive and robotics industries, as well as in traffic and fleet management. These devices are used in healthcare to keep track of patients and other assets in real time. A typical M2M architecture will consist of the M2M domain, the network domain, and the application domain.

3. IoT Layered Architecture



IoT World Forum Reference Model

Levels

7 **Collaboration & Processes** (Involving People & Business Processes)

6 **Application** (Reporting, Analytics, Control)

5 **Data Abstraction** (Aggregation & Access)

4 **Data Accumulation** (Storage)

3 **Edge Computing** (Data Element Analysis & Transformation)

2 **Connectivity** (Communication & Processing Units)

1 **Physical Devices & Controllers** (The "Things" in IoT)

Center
Edge
Sensors, Devices, Machines,
Intelligent Edge Nodes of all types
5

Fig.1 IoT Layered Architecture[3]

These parts form the foundation of an IoT system on which multi-layered architecture can be built. Most layers are: the perception layer hosting smart objects; the connectivity or transport layer transferring data from the physical layer to the cloud and vice versa via networks and gateways; the processing layer employing IoT platforms to accumulate and manage all data streams; and the application layer delivering end-user solutions such as analytics, reporting, and device control.

i. **Data Accumulation Layer :** This layer holds data for use by programmes. Converts event data to query processing. Application data can be stored in files, databases, or preferences on internal or portable storage. Statistics Data-authenticating networks transport data. Data moves. Prior to Level 4, data moves through the network at the rate and organisation set by the data-generating devices.

ii. **Data Abstraction Layer:** In short, the Internet of Things is disjointed. There are a lot of organisations who say they are the de facto worldwide connectivity standard for the Internet of Things. Because of this, developers of IoT apps and devices are placed in a catch-22 that ultimately threatens the health of the ecosystem. Providing a consistent abstract data model across all devices providing the same service, the Data Abstraction layer overcomes these obstacles and makes the implementation of connectivity independent of specific vendors, APIs, and protocols. A new device can be easily and dynamically incorporated using this way. Device-specific language binding scripts are used in the Data abstraction layer to provide translation rules. All the scripts are JSON-formatted text files. Once a device is recognised, these scripts are pulled from the Weaving Things cloud service and executed. Integralists are prone to using esoteric language. The rest of the translation work can be done with the help of a language abstraction script.

4. Cyber Attacks on IoT Layers

1. Data Accumulation Layer

a. **SQL Injection:** An attacker uses SQL injection to harm the database by inserting malicious SQL commands. Data can be compromised, altered, or even destroyed through SQL injection attacks. An SQL injection attack succeeds when a hacker assumes the identity of a user with limited access to the database, then modifies a lawful request with malicious code. The security of IoT devices is a major issue. As these gadgets require remote access, a firewall cannot be used to secure them. As a result, Internet-of-Things gadgets are open to attacks that computers and mobile phones might easily dodge[4].

b. **Ransomware**: Ransomware is malicious software that encrypts data in order to block access to a computer. Malware is a form of ransomware. Malware is used to encrypt the information. In many cases, the deadline for paying a ransom is set in stone. The ransom amount will either decrease or increase until the victim pays. As a result of the ease with which sophisticated viruses can manipulate devices with limited resources in an IoT environment, the entire network of physical devices can be shut down. Cyber threats, such as ransomware, compromise the security, authenticity, and availability of the Internet of Things[5].

c. **Malicious Attack:** When malware infects a computer, it performs malicious tasks without the user's permission. Spam, ransomware, command and control, and other forms of malware are all constrained by malicious software. Some virus attacks are so devastating that they make national news. The Operation Prowli malware campaign has gained widespread notoriety.

2. Data Abstraction Layer

a. **DDOS**: A denial-of-service (DoS) attack is a malicious attempt to disrupt the availability of a website or service in order to gain illegal end user access. In most cases, bushwhackers overwhelm the targeted system with a barrage of packets or requests. The bush hacker employs a variety of compromised or controlled sources to launch a distributed denial of service assault. As the OSI subcaste that a DDoS attack targets can be isolated. The Network, Transport, Donation, and Operation Layers see the most occurrences of these[6].

b. **Man in The Middle Attack**: A man- in- the- middle (MITM) attack disrupts a conversation or data transmission by eavesdropping or impersonating a legitimate participant. The target will perceive it as a normal information exchange, but the bushwhacker can still take information by inserting themselves in the middle. A MITM attack collects non-public data like as bank account information, credit card numbers, and login credentials for identity theft or illegal financial transfers. Because they occur in real-time, MITM attacks frequently go undiscovered until it is too late[7].

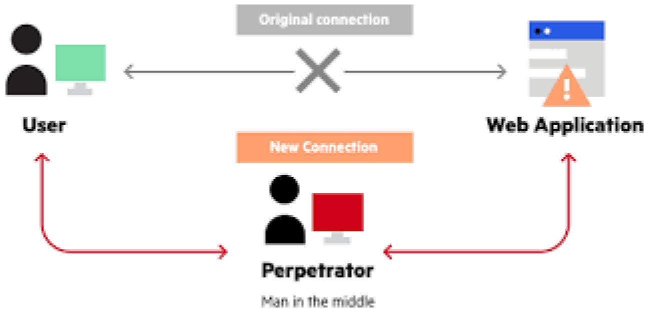


Fig. Man in middle attack

c. **Buffer Overflow**: When a programme or process attempts to store more information in a memory block (or buffer) than the buffer can hold, a buffer overflow occurs. Excess information leaks into neighbouring memory locations, corrupting or overwriting any data stored there. It's possible that hackers or stoned thugs may follow the directions in duplicate data and break lines, tamper with data, or reveal sensitive information. Hackers exploit buffer overflows to steal data from databases and stop applications from running. Produce safe legislation to forestall buffer overflow[8].

d. **Botnet**: A botnet attack occurs when a hacker infects a number of internet-connected computers with malicious software. Typically, it includes spam, data theft, exploitation, and DDoS attacks. Botnets exploit your prejudice to deceive others or cause disturbances without your permission. Bots automate attacks such as data theft, server breakdowns, and malware distribution. This exploit impacts database services such as MySql waiters[9].

e. **Reverse Engineering:** Reverse engineering involves disassembling an object to determine its purpose. Reverse Engineering is a person-to-person attack in which a bushwhacker informs the target that he or she has a problem, or will in the near future, and that he can help solve it. The hacker contacts the target via email and social media, employing multiple techniques and posing as a donor or security labour force to get network access. Although archaic and ridiculous, this strategy has proven effective, particularly when the victim's system or network is compromised. The information is used by hackers to attack an operation and its component programmes. Despite the fact that reverse engineering poses a significant threat to operations, many apps are submitted without security. In an analysis of 30 mobile fiscal applications, 97 lacked double protection, permitting the decompilation of source code[10].

f. **Brute Force Attack**: The Brute Force Attack is based on trial and error. Decodes secret data. Password and encryption key cracking are common uses. Passwords, login credentials, and encryption keys can be deciphered by trial-and-error methods. It is a simple method for gaining unauthorised access to accounts, systems, and networks. Various brute force approaches expose sensitive data in various ways[11].

g. **Spoofing Attack**: Spoofing involves disguising a message or identity as coming from a trusted, authorised source. Phishing-related email spoofing and phoney caller ID spoofing are two examples of spoofing attacks. Spoofing attacks may target the IP address, DNS server, or ARP service of a network[12].

Spoofing attacks imitate a trusted individual or organisation. In certain instances, such as with whale phishing attacks employing email spoofing or website spoofing, these messages may be tailored to the receiver in order to convince them that the communication is genuine. An individual who is unaware that internet communications can be forged is susceptible to spoofing.

4. Conclusion

In this paper, a complete description of cyber-attacks against Internet of Things systems was conducted, taking into account the systems' most critical characteristics and vulnerabilities. Our long-term objective is to do in-depth study on an even larger number of IoT systems, with a focus on the cyber security issues identified in this work and the creation of effective countermeasures. The purpose is to undertake research on various solutions that might be used to construct a fully modular infrastructure that can scale well for Internet of Things (IoT) systems on a wide scale.

References

[1] S. S., R. Somula, B. Parvathala, S. Kolli, S. Pulipati, and A. S. S. T., “SOA-EACR: Seagull optimization algorithm based energy aware cluster routing protocol for wireless sensor networks in the livestock industry,” *Sustain. Comput. Informatics Syst.*, vol. 33, p. 100645, 2022.

[2] “0a639f751f9d5ca1d50bc858f182174a25484472 @ www.ibm.com.” .

[3] “ce5f65e01c222664485808d8b21c1692652f954c @ www.altexsoft.com.” .

[4] “sql-injection @ portswigger.net.” .

[5] “210f72487c5ad1443e968144753f4160caf95e5c @ www.checkpoint.com.” .

[6] “f3640b02978d765d8d35a7537b14bb8e64048c23 @ www.cloudflare.com.” .

[7] “ac479c4bc3f4297a4343a3a2b76f75594a1b0b1a @ www.imperva.com.” .

[8] “cbc928eb8de1beef8ff359e9b2f4bf823734055d @ www.imperva.com.” .

[9] “f7c71a85fc4444c4e37667c164941c8d5f4a266e @ securityintelligence.com.” .

[10] “reverse-engineering-attacks-6-tools-your-team-needs-know @ techbeacon.com.” .

[11] “brute-force-attack @ www.kaspersky.com.” .

[12] “68c6dbf076746617a9700957504fe947f243030f @ www.rapid7.com.” .