IoT and Cyber Security: Introduction, Attacks, and Preventive Steps

Chapter · January 2020

DOI: 10.4018/978-1-7998-2253-0.ch010

2 authors, including:

NIRBHAY KUMAR CHAUBEY
Ganpat University
68 PUBLICATIONS **517** CITATIONS

SEE PROFILE

Chapter 10
IoT and Cyber Security: Introduction, Attacks, and Preventive Steps

Keyurbhai Arvindbhai Jani
https://orcid.org/0000-0002-6050-9365
U. V. Patel College of Engineering, Ganpat University, India

Nirbhay Chaubey
Acharya Motibhai Patel Institute of Computer Studies, Ganpat University, India

ABSTRACT

The Internet of Things (IoT) connects different IoT smart objects around people to make their life easier by connecting them with the internet, which leads IoT environments vulnerable to many attacks. This chapter has few main objectives: to understand basics of IoT; different types of attacks possible in IoT; and prevention steps to secure IoT environment at some extent. Therefore, this chapter is mainly divided into three parts. In first part discusses IoT devices and application of it; the second part is about cyber-attacks possible on IoT environments; and in the third part is discussed prevention and recommendation steps to avoid damage from different attacks.

INTRODUCTION

Nowadays technology changing rapidly day by day and affect our lives in many ways. Internet connectivity easily available everywhere. Many devices like computers, laptops, network devices, smartphones etc. connected with internet around us.

DOI: 10.4018/978-1-7998-2253-0.ch010

Popularity of the Internet of Things (IoT) has increase in last few years and number of applications for introduced in market for different IoT domain such as traffic controlling, home automation, transportation management, manufacturing management, environmental monitoring, defense system, medical industries, smart farming, etc. In different applications of IoT many sensors, actuators, Gateway, Circuits, hardware and routers communicate with each other via wired/wireless communication technologies are known as IoT devices. More than 50 billion IoT devices will connect with internet by 2020 as per Cisco white paper.

There are many communication technologies and way to connect anything(IoT devices) such as radio frequency identification (RFID), ZigBee, Bluetooth, Bluetooth low energy (BLE), wireless fidelity (Wi-Fi), worldwide interoperability for microwave access (WiMAX), wireless personal area network (WPAN), near field communication (NFC),Ethernet cables, coaxial cable, mobile communication technology (1G/2G/3G/4G/5G/GSM/CDMA) and many more that depends on existing infrastructure whether wired or wireless.

There are various protocols used in IoT such as advanced message queuing protocol (AMQP), constrained application protocol (CoAP), message queuing telemetry transport (MQTT), multicast domain name system (mDNS), domain name system service discovery (DNS-SD), extensible messaging presence protocol (XMPP), representational state transfer (RESTFUL) services, IPv6 over low-power wireless personal area networks (6LowPAN), internet protocol version 4 (IPv4)/ internet protocol version 6 (IPv6), routing protocol for low-power and lossy networks (RPL), HyperText transfer protocol (HTTP), web sockets and many more protocols being used at the different layers.

Security play vital role when these devices are near to us and send their data over network. IoT devices are also widely used in industries. Therefore, it is important to consider risk of cyber vulnerabilities & attacks in IoT environment and implementing recommendation steps to secure IoT environment to some extent.

Introduction to IoT

Many people and organizations gave different definitions of IoT. IoT is not a new concept. In previous era internet connect people so it has called “the Internet of People.” Few years ago, the internet was not widely available in industries, research institutes, and in the government sector. The concept of M2M, machine-to-machine, was introduced so machines can talk to each other with some wired or wireless technologies to take some collaborative decisions and perform some tasks. It is also famous as Sensor Network. Nowadays internet widely available to every person at low cost, therefore these IoT objects (cloud/web server/node/sensor/machine/app) has direct connectivity to the internet and send their data via internet to other

objects and all these IoT objects considered as Things, so it is called "the Internet of Things." Cisco gave its name as "Internet of Everything". Bruce Schneier gave it the name "World Size Web." In the *Terminator* movie, "Skynet," was the name given to the IoT concept.

Now, let us discuss more about things in IoT. Things are mainly identified as physical world objects and information world (virtual) objects. Things have unique identities and able to communicate with each other via communication layer. Physical things are surrounding environment, sensors, electrical-electronics equipment, actuators etc. whereas IoT applications (web/mobile app), Twitter, Facebook, Thingspeak, Blynk, etc., are virtual things, its capable of being stored, processed, and accessed.

Therefore, The IoT is a connected network of physical and virtual objects (Devices, vehicles, Buildings and other items embedded with electronics, software, web application, mobile application, sensors, and network connectivity, etc.) that enables these objects to collect and exchange data as per description given in (Wikipedia, n.d.). Therefore, as shown in Figure 1, IoT is environment, which connect people & process with physical/virtual objects (sensors) via some connectivity technologies.

In IoT by accessing IoT web/mobile applications like CRM system, remote monitoring/maintenance /supply chain management, location tracking, and many more people can take part as shown in Figure 2. E.g.: In location tracking applications, at some interval GPS sensors send its location data to its configured server, on server that data processed and stored in database, Mobile application & web app provide interface to user to access that data & do necessary action/decision based on application requirement.

Figure 1. IoT Environment components

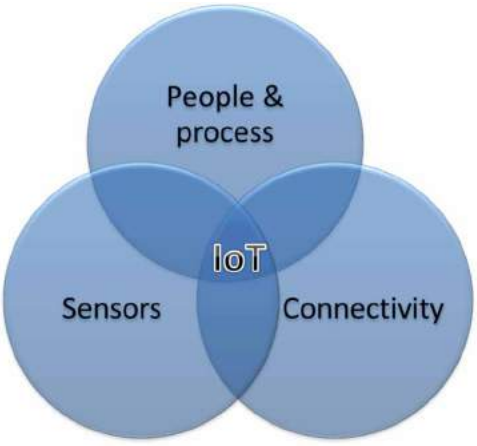
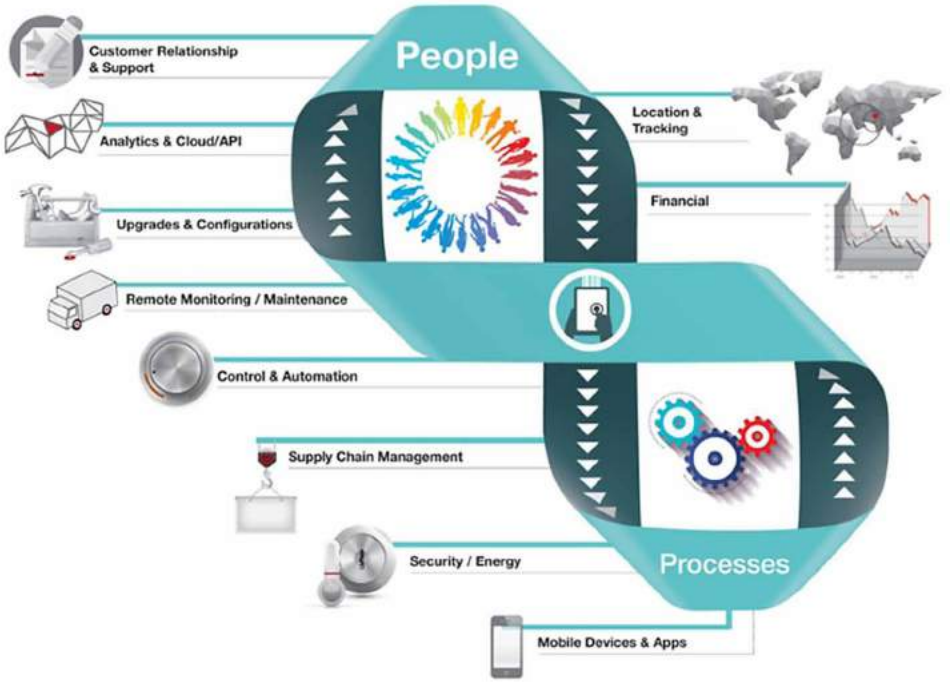


Figure 2. People & Process in IoT
Source: (Postscapes, n.d.)

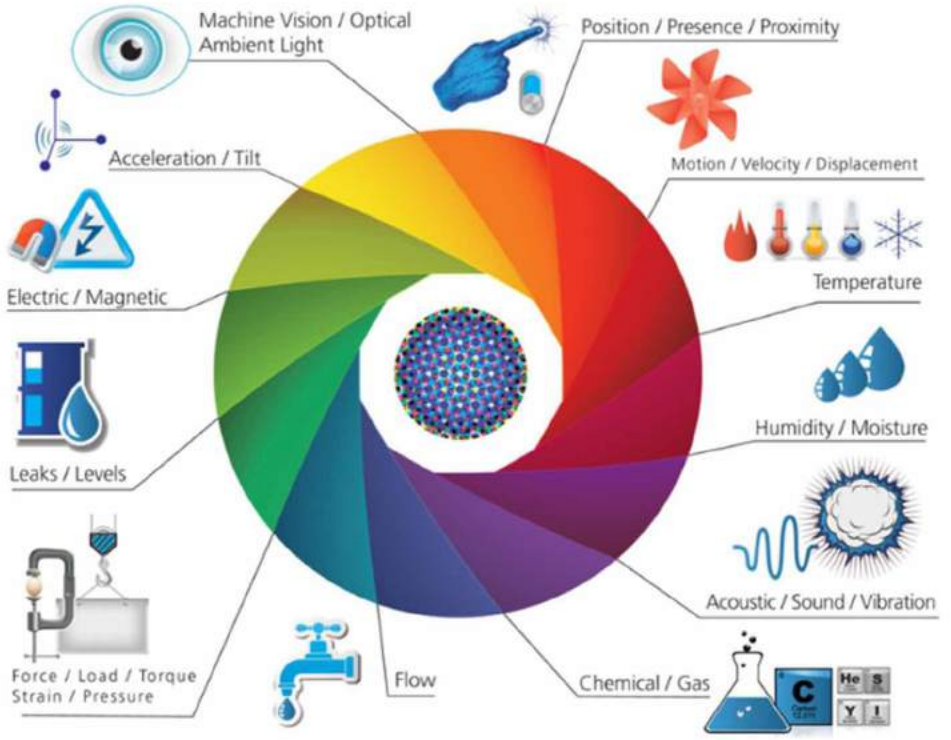


Sensors and actuators are core of IoT. There are many known sensors which are easily available in the market and widely used by people, government and industries as per application requirements as shown in Figure 3.

Few Sensors, Actuators, Development Boards and Power Supplies are described as below for reference:

- **Raspberry Pi:** Use it as development board, web server and gateway. Install Raspbian OS, Apache, PHP, MySQL server, FTP server and many more software. To develop a hardware level computer skill of school students in the UK, the Raspberry Pi Foundation, develops single-board computers with I/O pins. The University of Cambridge Computer Laboratory and tech firm Broadcom supports it. It's come with C, C++, Java, Scratch, and Ruby like software pre-installed in OS. Purpose behind choosing this name was the combination of the desire to create an alternative fruit-based computer (like Apricot, Blackberry, Apple) with the simple and very powerful programming language Python (shortened to Pi).

Figure 3. Sensors in IoT
Source: (Postscapes, n.d.)



- **Arduino:** With this development board, we can attach different sensors, actuators and communication devices. Developer can implement their logic with Arduino IDE, which uses C language type of syntax. Its open source project so there is strong developer communities and tutorials like resources easily available on the internet.
- **NodeMCU:** NodeMCU is an open source IoT platform. It is low cost development board based on ESP8266 with GPIO, PWM, IIC, 1-Wire and ADC all in one board which easily powered by your mobile charger (5v DC). The default firmware uses the Lua as a scripting language. It provides Arduino-like hardware IO, Nodejs style network API and lowest cost WI-FI. We can develop program in Arduino IDE also. In new NodeMCU, people can get advantages of WI-FI and Bluetooth also.
- **Bluetooth Module:** This communication device use for data transfer from Arduino, Raspberry Pi like board or microcontroller.

Figure 4. Raspberry Pi

Figure 5. Arduino

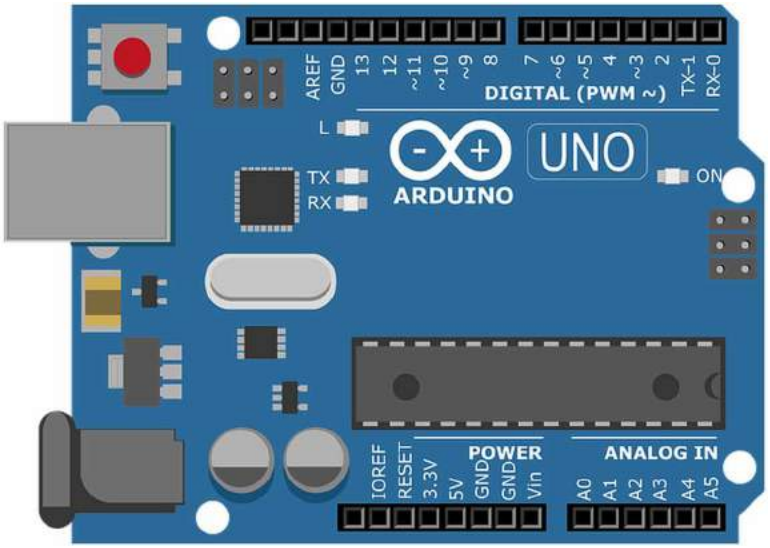
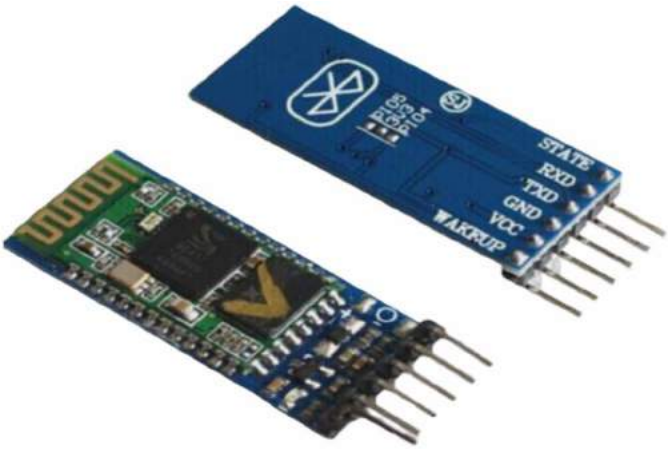


Figure 6. NodeMCU

Figure 7. Bluetooth Module (HC-05)



- **Solenoid Valve:** Used for automated water valve open close, here you can choose four type of water valve
  - 12v DC high pressure electric solenoid valve
  - 12v DC low pressure solenoid valve
  - 24v DC solenoid valve
  - 5v DC Modified brass ball valve for regulated water flow using servo motor
- **Water Flow Sensor:** These sensors are used to track information of water usages and leakages.
- **Ultrasonic Sensor:** Used as object distance detection sensor.
- **DHT (Digital Humidity Temperature):** These sensors use for measure temperature and humidity and give output in digital format.
- **Soil Moisture Sensor:** This sensor will give moisture level in soil.
- **Relay Module:** Use for AC/DC power switching.

Figure 8. Solenoid Valves

Figure 9. Water Flow Sensors

Figure 10. Ultrasonic Sensor

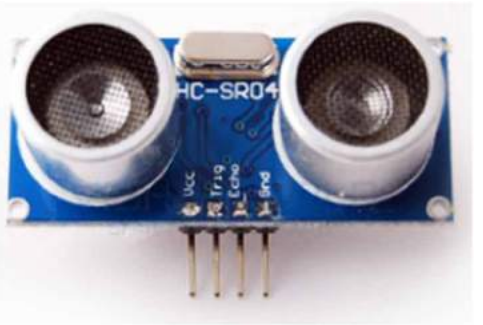
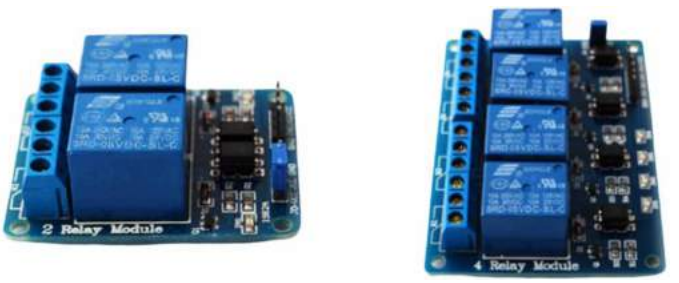


Figure 11. DHT 11 Sensor

Figure 12. Soil Moisture Level Sensor

Figure 13. Relay Modules



- **Breadboard Power Supply:** Some devices use 5V and some use 3.3V power for working. This will act as power source for Arduino and many sensors.
- **Step Up/Down DC-DC adjustable voltage regulator, SMPS, Power Adaptor, etc.**

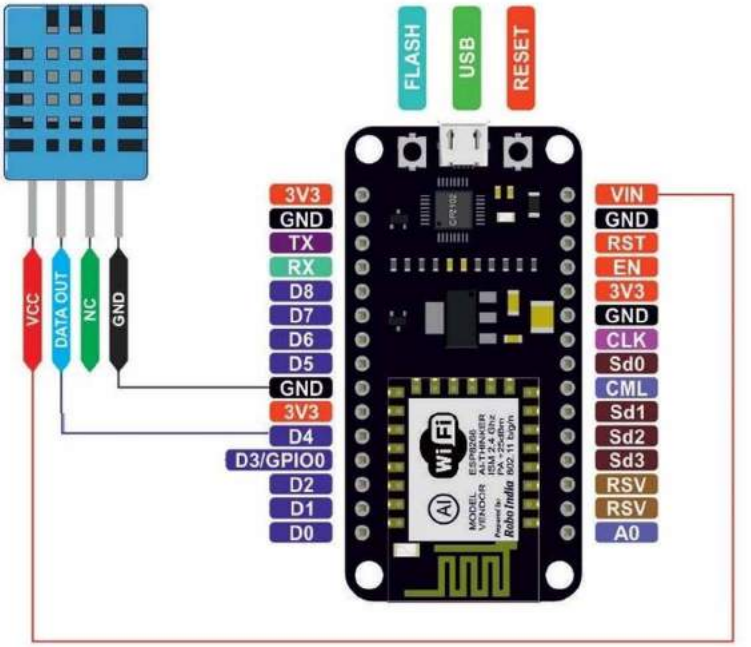
Figure 14. Breadboard power supply Module

- **Working with Sensors:** Most of sensors are not able to transfer data directly on internet or able to do process on sensed data. So, controller or development boards that have capability to do process on sensed data and transfer it to the server via internet are used in IoT application. To collect, process and store data, developers create web server or use cloud services. So, before discussing IoT architecture and all, let us take one example to understand simple IoT application with Thingspeak.com server (Website for storing, processing, analyzing and visualizing sensors data).
- **Experiment-1:** To sense environment temperature and humidity using DHT-11 sensor and upload data on thingspeak.com using NodeMCU.
- **Connection Diagram:** See Figure 15.

Steps to upload DHT data on thingspeak.com using NodeMCU:

1. Sign Up on www.thingspeak.com using your email id
2. Make sure to click the checkbox saying "By signing up, you agree to the Terms of Use and Privacy Policy
3. Goto Channels and Create a New Channel
4. Fill the following Details
   a. Any Name for the channel
   b. Description: if you have any description like "Monitoring temp and humanity"
   c. Field 1 Label as 'temp' and field2 label as humanity since we are going to upload temperature and humanity

Figure 15. NodeMCU-DHT11 Connection



5. Save Channel
6. Saving Process might take a while.
7. Please select your channel
8. You would see tabs Like
    a. Private View
    b. Public View
    c. Channel Settings
    d. API Keys
    e. Data Import/Export
9. Click API Keys Tab
10. You will find Write API Key similar to this “OHYNG8WWGHXXXXXX”
11. Please copy paste the API Key in your Project Code (NodeMCU, Arduino)
12. Once the Code is uploaded and the Arduino/NodeMCU starts running, Arduino/NodeMCU will upload the Temperature and Humidity value in few second gaps
13. Open Serial Monitor to see the process running in Arduino/NodeMCU
14. Click Private View Tab to see the graph.

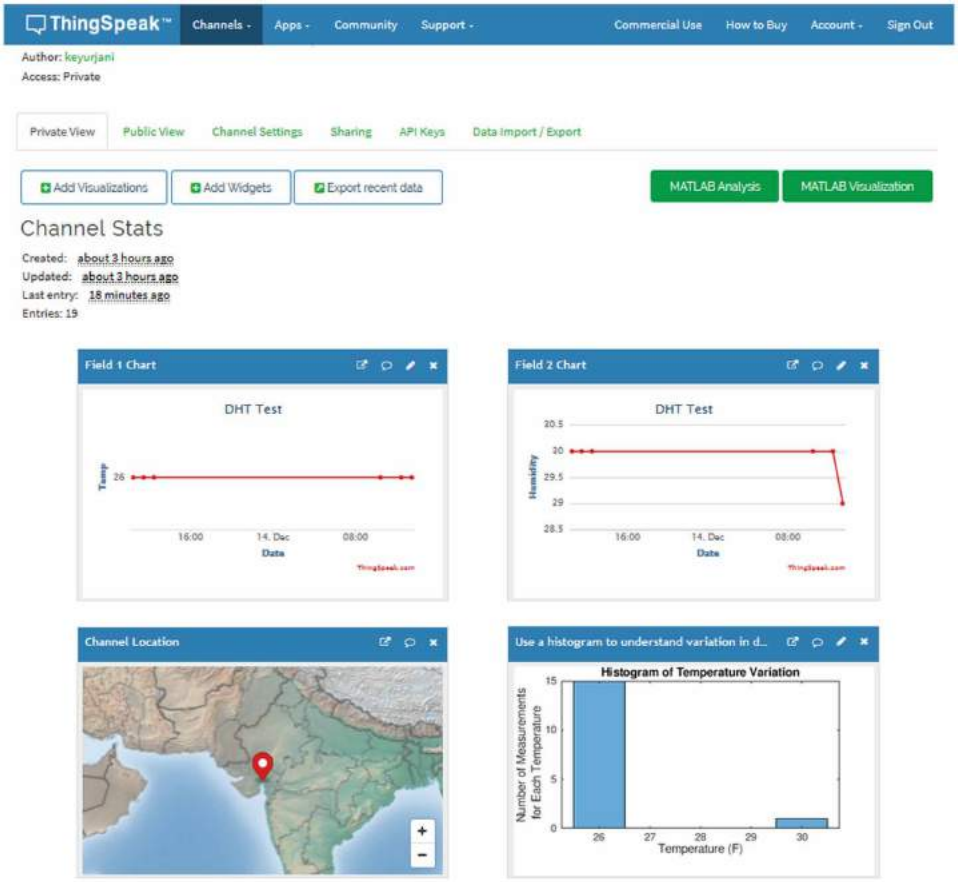
NodeMCU Code:

```
// Hardware: NodeMCU,DHT11
#include <DHT.h>  // this Include library for all known DHT
sensors
#include <Adafruit_Sensor.h>
#include <ESP8266WiFi.h>
String apiKey = "OHYNG8WWGHXXXXXX"; //replace your ThingSpeak
channel's //Write API key here
const char *wifi_ssid = "Your Wi-Fi Router/hotspot name";
const char *wifi_pwd =  "Your Wi-Fi Router/hotspot password";
const char* server = "api.thingspeak.com";
#define DHTPIN 2          //pin where the dht11 is connected D4
nodemcu
DHT dht(DHTPIN, DHT11);
WiFiClient client;
void setup()
{
       Serial.begin(9600);
       delay(100);
       dht.begin();
       Serial.println("Trying to Connect with ");
       Serial.println(wifi_ssid);
       WiFi.begin(wifi_ssid, wifi_pwd);
      while (WiFi.status() != WL_CONNECTED)
     {
            delay(5000);
            Serial.print("#");
     }
      Serial.println("");
      Serial.println("WiFi connected sucessfully");
}
void loop()
{
      float h = dht.readHumidity();
      float t = dht.readTemperature();
              if (isnan(h) || isnan(t))
                 {
                     Serial.println("Failed to read from DHT
sensor!");
```

```
                    return;
                }
             if (client.connect(server,80))
            {
                    String postStr = apiKey;
                    postStr +="&field1=";
                    postStr += String(t);
                    postStr +="&field2=";
                    postStr += String(h);
                    postStr += "\r\n\r\n";
                    client.print("POST /update HTTP/1.1\n");
                    client.print("Host: api.thingspeak.
com\n");
                    client.print("Connection: close\n");
                    client.print("X-THINGSPEAKAPIKEY:
"+apiKey+"\n");
                    client.print("Content-Type:application/
x-www-form-urlencoded\n");
                    client.print("Content-Length: ");
                    client.print(postStr.length());
                    client.print("\n\n");
                    client.print(postStr);
                    Serial.print("Temperature: ");
                    Serial.print(t);
                    Serial.print(" degrees Celcius,
Humidity: ");
                    Serial.print(h);
                    Serial.println("%. Send to
Thingspeak.");
                }
          client.stop();
          Serial.println("Waiting...");
  // thingspeak needs minimum 15 sec delay between updates,
i've set it         to 30 seconds
  delay(30000);
       }
```

- **Output:** See Figure 16.

Figure 16. Temperature & Humidity data on Thingspeak.com

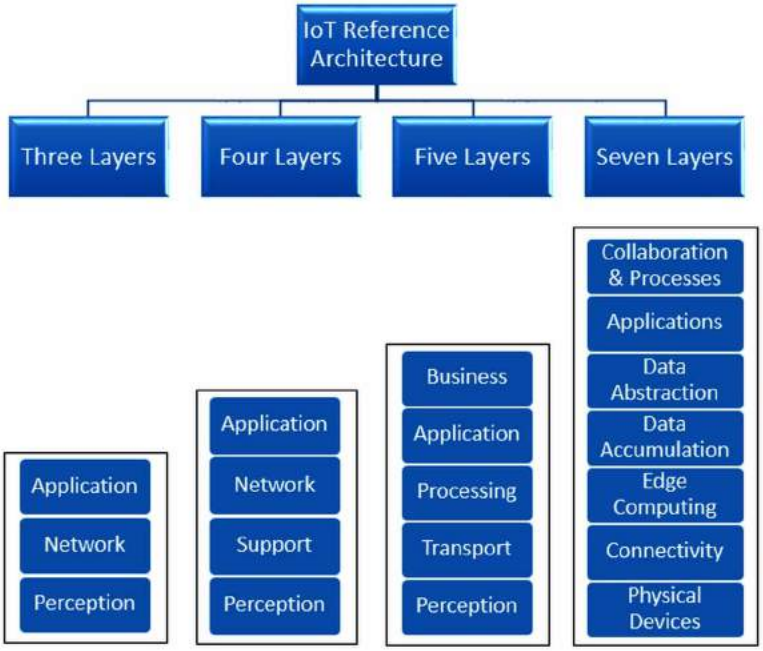


IoT Architecture

Different people describe IoT Architecture with different layers. Different researchers proposed different IoT Reference Models (RM) like: Three-level model (Abdul-Ghani & Konstantas, 2019), A Four-level model (Abdul-Ghan et al., 2018), a Five-level model (Atzori, Iera, & Morabito, 2010) and a Seven-level model (Cisco, 2014). Figure 17 shows few well-known IoT architectures layers as below:

Each layer provides some functionalities to upper and lower layer. To achieve interoperability, Industries people use standards of each layer. (Lee, 2016) Discussed each layer from seven layers architecture very well:

Figure 17. IoT Reference Models: 3/4/5/7 layers architecture



1. **Physical Devices:** This layer is 'T' (Things in IoT), alternatively called edge devices. It contains sensors, actuators, embedded systems, microcontrollers, cameras, RFID, Communication devices, hardware, power supplies, etc. Most of these physical devices has constrained resources (i.e., power source, processing, storage and communication interface) and use battery as the power source. However, based on the application requirement main power supply or battery power used. Power will be a limited resource, so most of the IoT Applications try to reduce power consumption of the nodes. In addition to numerous techniques to scale back the power consumption, IoT devices use low-power microcontrollers as we as low-power communication technologies. Most of the objects in IoT network has low-end microcontroller that has RAM, ROM and processing unit in it. Devices within the Perception Layer will be either static or mobile, however the proportion of mobile devices are smaller than the static ones (Arış, Oktuğ, & Voigt, 2018).
2. **Connectivity:** This layer provides an interface between physical layer and upper layers. It mainly consists communication related interface and protocols like (i.e., 6LoWPAN, Bluetooth Low Energy (BLE), LoRa and LoRaWAN, WiFi, Ethernet, Cellular, ZigBee, RF and Thread) which are used for the in-network communication. Most of them are open technologies, whereas a number of

them are (e.g., ZigBee, LoRa, Cellular) proprietary. These communication technologies give varied knowledge rates and transmission ranges reciprocally of various power consumptions and prices. Hence, depending on the several design constraints, the nodes in the Perception Layer can form IoT networks with different characteristics. Among these technologies, BLE, Wi-Fi, LoRa and Cellular offer star-based topologies. However, 6LoWPAN, ZigBee and Thread support mesh topologies, where elements of the network can forward others' packets. Some of them are projected for specific application areas (i.e., Thread was projected for smart-home environments). Most of these technologies require a gateway or border router, which used to connect the nodes in IoT network to the Internet (Arış, Oktuğ, & Voigt, 2018).

3. **Edge Computing:** The main objective of this layer is to perform simple data processing, which in turn decreases the computation load in the higher layers and offers a quick response. It is wise for real-time applications to process data closer to the edge of the network, rather than to process data in the cloud. Many factors (e.g., service providers and computing nodes) can be used to define the amount of data processing at this layer (Abdul-Ghani & Konstantas, 2019).
4. **Data Accumulation:** This layer given the Velocity, Volume and Variety that IoT systems can provide it is essential to provide incoming data storage for subsequent processing, normalization, integration, and preparation for upstream applications. While a part of the general "data lake" design, this layer of the design serves the intermediate storage of incoming storage and outgoing traffic queued for delivery to lower layers. This layer may be implemented in simple SQL or may require more sophisticated Hadoop & Hadoop File System, Mongo, Cassandra, Spark or other NoSQL solutions.
5. **Data Abstraction:** in this layer we have a tendency to "make sense" of the data, assembling "like" data from multiple IoT sensors or measurements, expedite high priority traffic or alarms, and organize incoming data from the information lake into acceptable schema and flows for upstream process. Similarly, application information destined for downstream layers is reformatted fittingly for device interaction and queued for process. A key design part for larger high-performance deployments could be a publish / subscribe or data distribution service (DDS) software package to modify data movement between Edge Computing, Data Accumulation, Application Layer, and User Processes (Lee, 2016). In general, this layer provides several functions such as normalization/renormalization, indexing, and access control to different data centers.
6. **Application:** In this layer, people see applications in various deployment areas, which make use of the meaningful information obtained from lower Layers. Applications of IoT can be in home, building, industry, urban or rural

environment Monitoring, process optimization, alarm management, statistical analysis, control logic, logistics, consumer patterns, are just a few examples of IoT applications (Arış, Oktuğ, & Voigt, 2018) (Lee, 2016).

7. **Collaboration and Processes:** At this layer, application processing is presented to users, and data processed at lower layers is integrated into business applications. This layer is concerning human interaction with all of the layers of the IoT system and wherever quantity is delivered. The challenge at this layer is to effectively leverage the worth of IoT and also the layers of infrastructure and services below and leverage this into economic process, business improvement and/or social good.

Table 1. Few IoT protocols

Protocols	Purpose
CoAP	CoAP is designed in such a way that it enables the low-power sensors to make usage of restful services It is built upon the UDP instead of the TCP that is commonly used in HTTP.
DDS	It provides an excellent quality of service levels and reliability that suits the IoT and M2M communication.
MQTT	It facilities the embedded connectivity between applications and the middleware at one side and networks and communications on the other
SMQTT	In this, one message is encrypted but delivered to multiple other nodes.
AMQP	In this, the broker is divided into two main components that are exchange and queues.
6LoWPAN	6LoWPAN is designed to work with variant length addresses, various network topologies including mesh and star, low bandwidth, scalable networks, mobility, and low cost
RPL	Routing Protocol for Low-Power and Lossy Networks (RPL) supports data link protocol
CORPL	An extension of RPL is CORPL or cognitive RPL, which is designed for the cognitive networks and uses DODAG topology generation.
CARP	A distributed routing protocol is designed for the underwater Communication. It has lightweight packets.
6TiSCH	A 6TiSCH working group in IETF is developing standards to allow IPv6 to pass through Time- Slotted Channel Hopping (TSCH) mode of IEEE 802.15.4e data links.
LTE-A	LTE-A is a scalable, lower- cost protocol as compared to other cellular protocols
Z-WAVE	Z-Wave is a low-power MAC protocol that is designed for home automation
IEEE 802.11 AH	IEEE 802.11ah is a low energy version of the original IEEE 802.11 wireless medium access standard.
Zigbee Smart Energy	It is designed for a broad range of IoT applications including Smart homes, remote controls, and healthcare systems. It supports a wide star, peer-to-peer or cluster-tree topologies.

Source: (Masoodi, Alam, Siddiqui, & Liz, 2019)

IoT Protocols

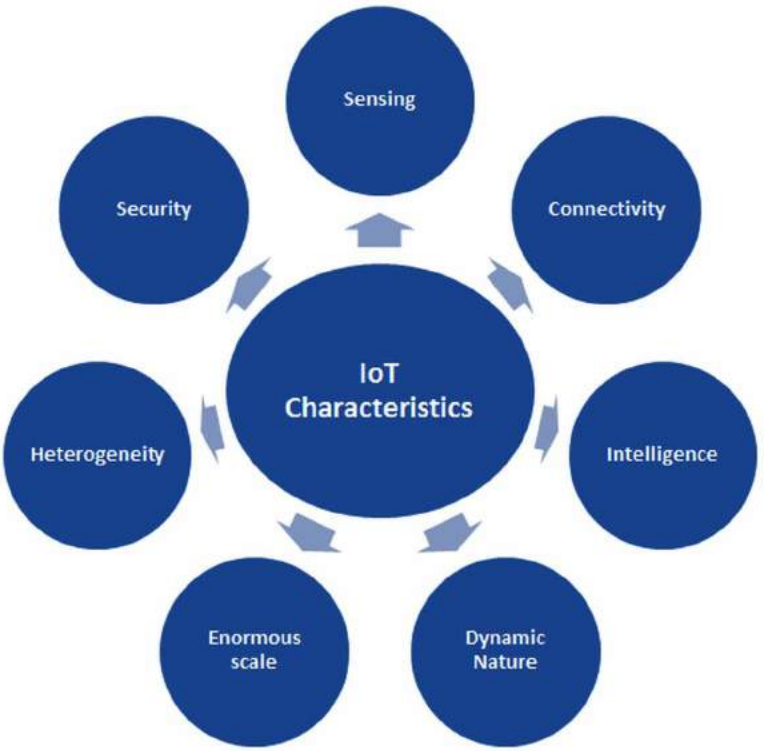
Table 1 shows a few protocols that are discuss by (Masoodi, Alam, Siddiqui, & Liz, 2019) at different layers of IoT architecture.

IoT Characteristics

IoT is a complex system with a number of characteristics. Characteristics vary from one domain to another in IoT. Few general and key characteristics are described by (Chandrashekhar, 2016) as follows:

1. **Sensing:** IoT would not be possible without sensors, which will detect or measure any changes in the environment to generate data that can report on their status or even interact with the environment. Sensing technologies give the means that to make capabilities that replicate a real awareness of the physical world and the folks in it. The sensing information is simply the analogue input from the physical world, but it can provide a rich understanding of our complex world.

Figure 18. IoT characteristics



2. **Connectivity:** It empowers Internet of Things by bringing together everyday objects. Connectivity of those objects is crucial as a result of straightforward object level interactions contribute towards collective intelligence in IoT network. It allows network accessibility and compatibility within the things. With this connectivity, the networking of smart things and applications can create new market opportunities for Internet of things.
3. **Intelligence:** IoT comes with the combination of algorithms and computation, software & hardware that makes it smart. Ambient intelligence in IoT enhances its capabilities that facilitate IoT Objects to retort in an intelligent way to a specific scenario and supports them in completing specific tasks. In spite of all the popularity of smart technologies, intelligence in IoT is only concerned as a means of interaction between devices, while user and device interaction is achieved by standard input methods and graphical user interface.
4. **Dynamic Nature:** The primary activity of Internet of Things is to gather information from its surroundings, this is often achieved with the dynamic changes that turn up nearer to the devices. The state of those devices change dynamically, for instance sleeping and awakening, connected and/or disconnected in addition because the context of devices change together with temperature, location and speed. In addition to the state of the device, the quantity of devices additionally changes dynamically with an individual, place and time.
5. **Enormous Scale:** The quantity of devices that require to be managed which communicate with one another are abundant larger than the devices connected to the present internet. The management of information generated from these devices and their interpretation for application functions becomes a lot of essential. Gartner (2015) confirms the big scale of IoT within the estimated report wherever it explicit that 5.5 million new things can get connected each day and 6.4 billion connected things are in use worldwide in 2016, that is up by 30% from 2015. The report conjointly forecasts that the quantity of connected devices can reach 20.8 billion by 2020.
6. Heterogeneity: Heterogeneity in IoT as one of the key characteristics. Devices in IoT are supported completely different hardware platforms and networks and may move with different devices or service platforms through different networks. IoT design ought to support direct network connectivity between heterogeneous networks. The key style needs for heterogeneous things and their environments in IoT are interoperability, scalabilities, modularity and extensibility.
7. **Security:** IoT devices are naturally vulnerable to security threats. As we tend to gain efficiencies, novel experiences, and alternative edges from the IoT, it would be an error to ignore security issues related to it. There is a high level

of transparency and privacy problems with IoT. It is necessary to secure the endpoints, the networks, and also the information that's transferred across all of it suggests that making a security paradigm.

IoT Applications

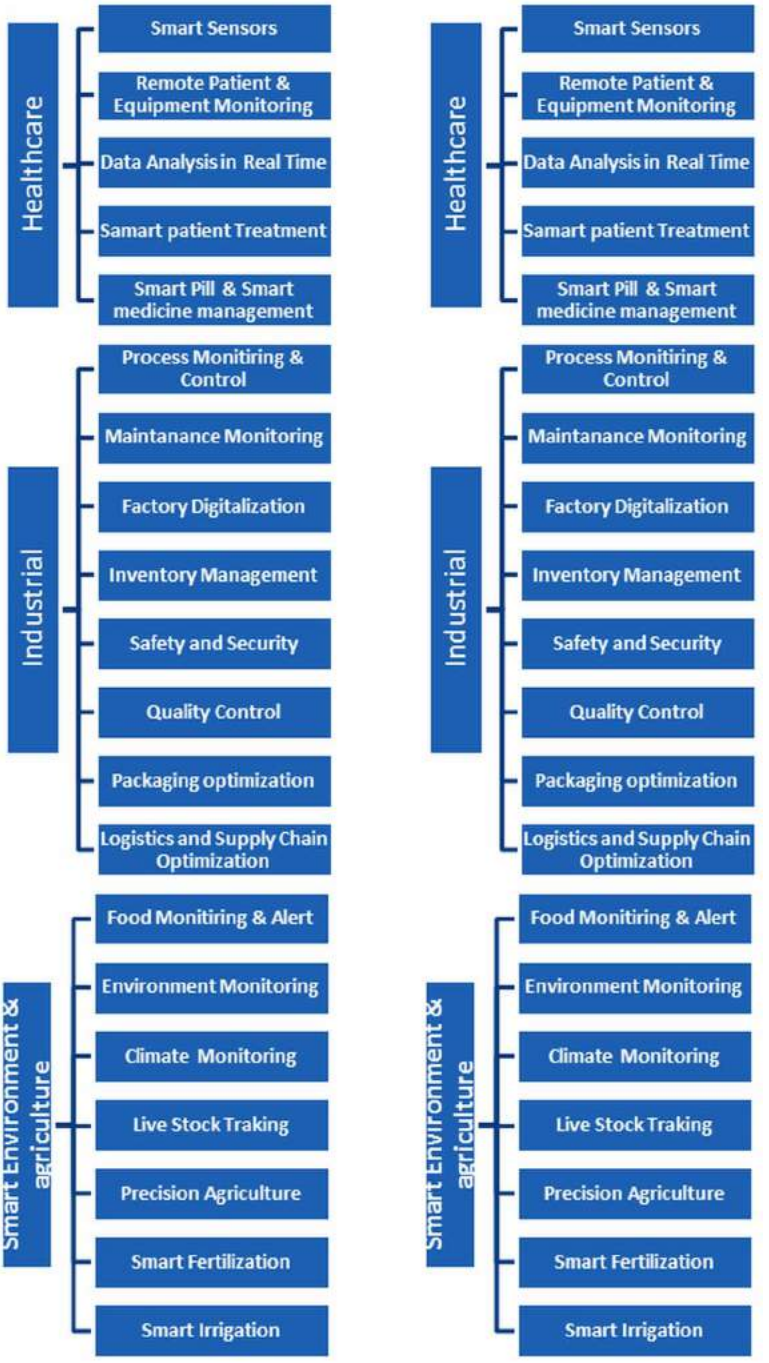
IoT has several applications. In Figure.19 Application divided domain wise. IoT applications connects billions of smart objects every day in different domain. Few key applications from every domain as below:

In Consumer domain Smart Home, Smart Cities, Smart building, Elder care, Wearables, Smart Gym & Museum type of applications are there. Even Smart Home contains lot of small application in it, which includes smart lighting, smart heating and air conditioning, smart media and smart security systems. Therefore, by implementing Smart Home we can make our life easy, secure and most important we can save valuable energy by smartly controlling it. However, if it can introduce significant risk to security and privacy. Attackers can directly compromise home devices, thereby undermining the user's security and privacy (Kumar & Patel, 2014). In many existing SmartApps, its communication with the device is accomplished by event. Due to the lack of sufficient protection, attackers can easily obtain sensitive information of users. Moreover, many of the existing development frameworks of SmartApps have vulnerabilities, and attackers can use these vulnerabilities to achieve a variety of attacks (Arias, Ly, & Jin, 2017) (Fernandes, Jung, & Prakash, 2016). Smart Cities also include Smart Parking, Smart lighting, Smart Traffic monitoring, Smart Road, Structural Health Monitoring etc.

In Utilities domain, also IoT has many applications like Smart Metering, smart grid, workforce Tracking, Asset and inventory management etc. Smart Grid integrated with electrical energy field. It collect electricity generation, Consumption, Storage & equipment's health status data. This data can be used for smart power distribution, faultfinding and prediction of usages. IoT also used for tracking asset and workforce for better management of it.

In Transportation & logistics domain IoT applied in Assisted Driving, Mobile Ticketing, Fleet Management & goods Tracking, Smart Traffic control, Smart parking, Electronic Toll Collection System, Remote Vehicle Control etc. Using IoT authorized person can track their asset as well as vehicle. Even in case of theft case they can control vehicle functionalities. In case of traffic system can find alternate route and suggest it for on time delivery in supply chain management system. In toll both there are RFID reader connected with software which detect smart tag (RFID tag) on vehicle and automatically debit money from account.

Figure 19. IoT applications



In healthcare domain IoT used with Smart Sensors, Remote patient monitoring, Medical equipment monitoring, Real time data analysis and alert system, Wearable devices, Smart patient treatment, Telemedicine, Smart pill, Smart medicine management system etc. To diagnose patient condition many sensors like: body temperature, blood pressure, electrocardiogram (ECG), heart rate, pulse oximeter oxygen saturation (SPO_2), patient movement, bed occupancy, etc., continuously sense data and send it to patient monitoring system which show history as well as alert in case of an any emergency.

In Industrial IoT application Process monitoring and control, equipment monitoring and maintenance, Quality control system, Safety and Security, Supply chain management and inventory management and many more are there. Using different sensors, actuators and devices most of industrial requirement can be manageable by IoT implementation.

Smart environment and agriculture applications are food monitoring and alert, air pollution monitoring, weather monitoring, noise pollution monitoring, forest fire detection, river flood detection, agriculture products livestock tracking, precision agriculture, smart irrigation, smart fertilization, etc., so with help of IoT implementation in above application we can improve quality of environment and agriculture product, take appropriate decision and able to save valuable resources.

IoT Stakeholders

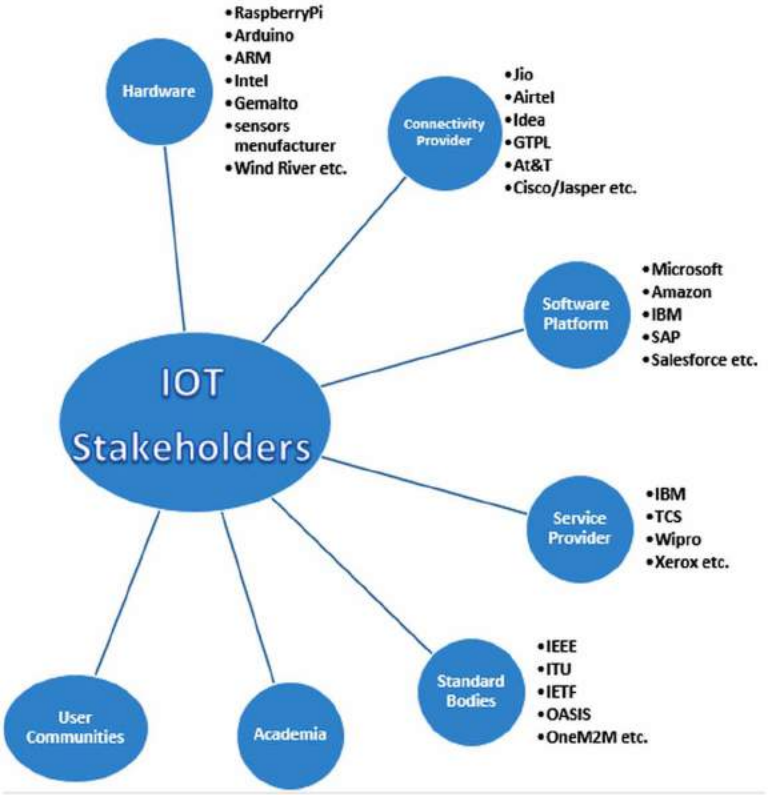
In IoT development many stakeholders play important roles. Below are few of them:

- **Hardware:** The hardware manufacturer is one of the key stakeholders who builds devices which used for developing IoT application. Different sensors, microcontroller, development board electronic actuators, etc., manufacture companies are key player and responsible for improving quality and security of IoT. It is duty of manufacturers to disclose their security support commitment to users prior to purchase.
- **Connectivity Provider:** Connectivity play major role in IoT. Without internet service providers (ISPs) the IoT applications can work just like WSN network. To work at its full potential ISPs provide infrastructure for it. To provide secure IoT environment they also play important role by securing their services. Ex: To prevent Botnet attack, several countries including Australia and Germany, ISPs block botnets emanating from residential IP addresses.
- **Software Platform:** Companies who provide software platform for developing IoT software, cloud services, server platform, etc., are also stakeholder of IoT. Many attacks done from vulnerabilities in this software platform so it is duty

of software platform companies to take care of it and provide solution to protect its product.

- **Service Provider:** Many Companies Provide different IoT services (hardware, software, server, Cloud etc.). Some time there are some security hole in their service so it duty of them to check frequently for security hole in their service and provide patch to protect IoT environment.
- **Standard Bodies:** Various organizations develop or approve standards for IoT platforms. Other IoT stakeholders follow standards for interoperability and secure environments.
- **Academia:** Universities and research organization are also one of the stakeholders for IoT development. They invent new technology or improve existing IoT technologies for efficient and secure IoT environment.

Figure 20. IoT stakeholders



- **User Communities:** Users are the basic stakeholder for IoT platform development. Due to user requirements, IoT applications develop. There are many attacks possible due to users careless, so users have to follow some recommendation to secure their IoT platform and if there are some vulnerabilities in IoT application its duty of user to give feedback to developer or authorities.

IoT Security Goals

To make IoT environment secure (Abdul-Ghani & Konstantas, 2019) discuss, all IoT components must try to achieve below security goals:

- **Confidentiality:** Is about keeping data private, so that only authorized users (both humans and machines) can access that data. Cryptography is a key technology for achieving confidentiality (Lin & W. Bergmann, 2016).
- **Integrity:** Is the process in which data completeness, and accuracy is preserved (Abdul-Ghani & Konstantas, 2019).
- **Non-Repudiation:** Is the process in which an IoT system can validate the incident or non-incident of an event
- **Availability:** Is an ability of an IoT system to make sure its services are accessible, when demanded by authorized objects or users.
- **Privacy:** Is the process in which an IoT system follows privacy rules or policies and allowing users to control their sensitive data.

Figure 21. IoT security goals

- **Audibility:** Is ensuring the ability of an IoT system to perform firm monitoring on its actions.
- **Accountability:** Is the process in which an IoT system holds users taking charge of their actions.
- **Trustworthiness:** Is ensuring the ability of an IoT system to prove identity and confirm trust in third party.

Possible Attacks

The Internet of things applications are used by many users but at the same time can expose the users to unprecedented security threats and challenges. Most of the IoT Devices directly connected with internet and share its data with some level of trust without performing any security tests. So most of attacks which are there in cyber space are also possible in IoT. IoT use Wireless Sensor Network as base so attacks of WSN are also there in IoT environment. Below are few attacks possible at different layers of IoT architecture discuss by (Abdul-Ghani & Konstantas, 2019) and (Chen et al., 2018).

Few of above attacks describe below to understand nature of attacks, which do damage at different layers of IoT environment:

- **Hardware Trojan**: One of the major security issues for ICs is hardware Trojans. They maliciously modify ICs to allow attackers to exploit their functionalities and gain access to software operating on them.

Table 2. Possible attacks at IoT architecture layers

Layer	Possible Attacks
Edge / Physical	Hardware Trojan, Node Replication, DoS Attacks (Sleep Deprivation, Battery Draining, Outage Attack), Physical Attack, Malicious Node, Side Channel Attack, Eavesdropping, Sniffing Attacks, Noise in data, Replay attack, etc.
Communication/ Network	Side Channel Attack, Collision Attack, Fragmentation Attack, Routing Attacks (Hello packet flood, Gray Hole, Sybil Attack, Worm Hole, Selective Forwarding, Black Hole, etc.), Eavesdropping, Inject Malicious Packets, Unauthorized Conversation, DoS attacks, Desynchronized attack, etc.
Middle layers	Web Browser attack, Signature Wrapping attack, Cloud Malware Injection, Flooding attack on cloud/server, SQL Injection, etc.
Application, Collaboration and Processes	Code Injection, Buffer Overflows, Phishing Attack, Authentication & Authorization, Private data Hijacking, Tampering with Node-based application, Application Security hole, Remote configuration, etc.

- **Node Replication:** The main goal of such an attack is to add maliciously an object by duplicating one object's identification number to a current set of objects. A remarkable drop in network performance can happen because of this attack. Furthermore, upon arrival of packets at a replica, it may not only corrupt the packets, but also misdirect them, causing serious damage to IoT systems by allowing an attacker to gain access to security parameters (e.g., shared keys). It is also capable of revoking authorized nodes, since it can carry out an object-revocation protocol (Parno, Perrig, & Gligor, 2005).
- **Denial of Service (DoS) Attacks:** DoS attacks in computing nodes can be classified into three categories: sleep deprivation, outage, and battery draining attacks at edge layer. In sleep deprivation, battery-operated node may receive a huge number of requests, which look like legitimate ones, sent by an attacker. Some IoT device work on battery. Battery draining attack are extremely powerful, leading to harmful impacts, such as a power outage. Outage attacks takes place when an IoT object stops carrying out its essential functions. This might have happened due to undesired error in the manufacturing phase, sleep deprivation, and code injection (Chaubey, Akshai Aggarwal, & Jani, 2015) (Chaubey, 2016).
- **Physical Attack:** In some IoT Application objects deployed in hostile environments, such objects are vulnerable to physical access, which may lead to hardware/firmware attacks. With physical access to an object, an attacker can derive precious cryptographic information, alter operating system, and vandalize circuit, all of which may result in long-term destruction.
- **Malicious Node:** In IoT environment, some node obtaining unauthorized access of an IoT network and other objects, and disturb functionalities and security of environment (Aggarwal, Chaubey, & Jani, 2013), (Chaubey, Aggarwal, Gandhi, & Jani, 2015).
- **Side Channel Attacks:** It is a strong attack against encryption techniques, which may affect their security and reliability. In Side-channel attack at edge node level objects perform their normal operations, there is a possibility that such objects might disclose critical information, side-channel attacks at communication level are not invasive, since they only elicit intentionally leaked information.
- **Collision Attacks:** This type of attacks can be launched on the link layer. One way is by adding noise in communication channel, which lead to retransmission of packets and drainage of limited power resources.
- **Fragmentation Attacks:** Although 6LoWPAN lacks any security mechanisms, its security is offered by underlying layers (e.g., an IEEE 802.15.4). The IEEE 802.15.4 has Maximum Transmission Unit (MTU) of 127 bytes, whereas IPv6 has a minimum MTU of 1280 bytes. Being

developed with fragmentation technique, 6loWPAN provides the transfer of IPv6 packets over IEEE 802.15.4. In this case, an attacker can insert a malicious packet among other fragments, as 6loWPAN has designed without authentication techniques given by (Tomic & McCann, 2017).

- **Routing Attacks:** To transfer data in IoT environment many routing protocols used in network. Malicious node modified packet, generate fake packets, modify route. As per literature study, there are Sybil, Gray Hole, Wormhole, Hello flood, and Selective-forwarding types of attacks are possible in it (Aggarwal, Chaubey, & Jani, 2013), (Patel, Aggarwal, & Chaubey, Analysis of Wormhole Attacks in Wireless Sensor Networks, 2018) and (Patel, Aggarwal, & Chaubey, 2017).
- **Unauthorized Conversation:** To share and access data, each IoT object requires to communicate with other objects. That said, each object must only interact with a set of objects, which need its data. This kind of restricted interactions will prevent unauthorized access to IoT objects that is a fundamental security requirement of IoT. For instance, a thermostat, in a smart home, depends heavily on a smoke detector's data to turn a heating system off in case of danger. Nevertheless, insecurely sharing data with other objects by the smoke detector may put the entire smart home at risk (Mosenia & Jha, 2017).
- **Flooding Attack in Cloud**: This is one form of denial-of-service attacks in the cloud. Here, attackers constantly send requests to a service in the cloud, which depletes the resources in the cloud, thereby affecting the quality of service. When the cloud system finds that the current service instance cannot meet the requirements; it will transfer the affected service to other servers. This will lead to increased work pressure on other servers (Chen et al., 2018).
- **Cloud Malware Injection:** The attacker can modify the data, obtain control, and execute malicious code by injecting malicious service instance or virtual machine into the cloud.
- **Signature Wrapping Attack:** Cloud system uses XML signature to ensure the integrity of the service. The attacker modifies the eavesdropped messages without invalidating the signature. Some cloud use SOAP Attackers exploit vulnerabilities in SOAP to modify eavesdropped messages (Chen, et al., 2018).
- **SQL Injection Attack:** Attackers use web or mobile application interface to fire SQL statements for reading, writing, and deleting operations. This kind of attack can not only obtain the user's private data but also threaten the entire database system. When Web applications are attacked by SQL injection, the current page shows different outcomes compared to the true information discussed by (Chen et al., 2018) and (Dorai, 2011).

The attacks in the application layer mainly target (unauthorized) access of sensitive data of the user. Attackers typically exploit the vulnerabilities of programs and application (e.g., code injection, buffer overflow), or unauthorized access to attack. One approach for an unauthorized agent to obtain the same permission as legitimate users is through counterfeiting identity. In addition to these attacks, viruses, worms, and Trojans also threaten the application layer. Furthermore, other malicious programs (Rootkit, spyware, adware, etc.) also undermine the privacy of users.

Preventive Steps

Most of the above attacks are possible due to improper configuration & not following certain standards in IoT environment. Many organizations work for assessing security and providing guidelines for secure setup of IoT environment. The OWASP (Open Web Application Security Project) work on some security issue and come with Internet of Things Project which is designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies. OWASP and (Pal, n.d.) suggested some common issues in IoT applications and countermeasure steps to secure it.

FUTURE RESEARCH DIRECTIONS

As seen above in this chapter, there are various applications of IoT in market with different functionalities. Many applications have their own vulnerabilities and lack of following standards at each layer. In addition, IoT environment connected with internet so all threats related to cyber can be also applicable to IoT, therefore continuous software and firmware patch shall be produced for IoT applications are necessary to protect it. Many new technologies, protocols, hardware and communication devices research require to develop and secure IoT environment.

CONCLUSION

In this chapter, author discuss about IoT, which is fastest growing technology now days and much research is going on in this domain. IoT makes people's lives easier with its variety of applications. To do this task most of IoT objects use internet so they are directly vulnerable with internet threats. Therefore, to make IoT environment secure all IoT stakeholders have to do collaborative efforts by following standards and have to work towards improvement of standards and security for IoT environment.

Table 3. Common issues, reasons and prevention steps

Issue	Reasons for Issue	Prevention Steps
Poor Physical Security Weaknesses are present when an attacker can disassemble a device to easily access the storage medium and any data stored on that medium. Weaknesses are also present when USB ports or other external ports can be used to access the device using features intended for configuration or maintenance. This could lead to easy unauthorised access to the device or the data.	• Access to Software via USB Ports • Removal of Storage Media.	Ensure following • Data storage medium cannot be easily removed • Stored data is encrypted at rest • Device cannot be easily disassembled • USB ports or other external ports cannot be used to maliciously access the device • Only required external ports such as USB are required for the product to function • The product has the ability to limit administrative capabilities.
Insecure Software/Firmware Devices should have the ability to be updated when vulnerabilities are discovered and software/ firmware updates can be insecure when the updated files themselves and the network connection they are delivered on are not protected. Software/ Firmware can also be insecure if they contain hardcoded sensitive data such as credentials. The inability of software/ firmware being updated means that the devices remain vulnerable indefinitely to the security issue that the update is meant to address. Further, if the devices have hardcoded sensitive credentials, if these credentials are exposed, then they remain so for an indefinite period.	• Encryption Not Used to Fetch Updates • Update Not Verified before Upload • Update File not Encrypted • Firmware Contains Sensitive Information • No Update functionality or OTA option	Ensure following • The device has the ability to update • Update file is encrypted using accepted encryption methods • Update file is transmitted via an encrypted connection • Update file does not expose sensitive data • Update is signed and verified before allowing the update to be uploaded and applied • Update server is secure.
Insecure Network Services This relates to vulnerabilities in the network services that are used to access the IoT device that might allow an intruder to gain unauthorized access to the device or associated data.	• Vulnerable Services • Buffer Overflow • Open Ports via UPnP • xploitable UDP Services • Denial-of-Service • DoS via Network Device Fuzzing	Ensure following • Services are not vulnerable to buffer overflow and fuzzing attacks • Only necessary ports are exposed and available • Services are not vulnerable to DoS attacks which can affect the device itself or other devices and/or users on the local network or other networks • Network ports or services are not exposed to the internet via UPnP for example
Lack of Transport Encryption This deals with data being exchanged with the IoT device in an unencrypted format. This could easily lead to an intruder sniffing the data and either capturing this data for later use or compromising the device itself.	• Unencrypted Services via the Internet • Unencrypted Services via the Local Network • Poorly Implemented SSL/ TLS • Misconfigured SSL/TLS	Ensure following • Data is encrypted using protocols such as SSL and TLS while transiting networks • Other industry standard encryption techniques are utilised to protect data during transport if SSL or TLS are not available • only accepted encryption standards are used and avoid using proprietary encryption protocols
Insufficient Authentication/ Authorization Its due to ineffective mechanisms being in place to authenticate to the IoT user interface and/or poor authorization mechanisms whereby a user can gain higher levels of access then allowed	• Lack of Password Complexity • Poorly Protected Credentials • Lack of Two Factor Authentication • Insecure Password Recovery • Privilege Escalation • Lack of Role Based Access Control	Ensure following • The strong passwords are required • Granular access control is in place when necessary • Credentials are properly protected • Implement two factor authentication where possible • Password recovery mechanisms are secure • Re-authentication is required for sensitive features • Options are available for configuring password controls

continued on following page

Table 3. Continued

Issue	Reasons for Issue	Prevention Steps
Insecure Web Interface Web interfaces built into IoT devices that allows a user to interact with the device, but at the same time could allow an attacker to gain unauthorized access to the device.	• Weak Default Credentials • Account Enumeration • Credentials Exposed in Network Traffic • Cross-site Scripting (XSS) • SQL-Injection • Session Management • Weak Account Lockout Settings	Ensure following • Default passwords and ideally default usernames to be changed during initial setup • Password recovery mechanisms are robust and do not supply an attacker with information indicating a valid account • Web interface is not susceptible to XSS, SQLi or CSRF • Credentials are not exposed in internal or external network traffic • Weak passwords are not allowed • Account lockout after 3 -5 failed login attempts
Privacy Concerns It generated by the collection of personal data in addition to the lack of proper protection of that data. Privacy concerns are easy to discover by simply reviewing the data that is being collected as the user sets up and activates the device. Automated tools can also look for specific patterns of data that may indicate collection of personal data or other sensitive data.	• Collection of Unnecessary Personal Information	Ensure following • only data critical to the functionality of the device is collected • Any data collected is of a less sensitive nature • Any data collected is de-identified or anonymized • any data collected is properly protected with encryption • Device and all of its components properly protect personal information • Authorized individuals have access to collected personal information • Retention limits are set for collected data • End-users are provided with “Notice and Choice” if data collected is more than what would be expected from the product.
Insufficient Security Configurability It is present when users of the device have limited or no ability to alter its security controls. Insufficient security configurability is apparent when the web interface of the device has no options for creating granular user permissions or for example, forcing the use of strong passwords. The risk with this is that the IoT device could be easier to attack allowing unauthorised access to the device or the data	• Lack of Granular Permission Model • Lack of Password Security Options • No Security Monitoring • No Security Logging	Ensure the ability to as following • Separate normal users from administrative users • Encrypt data at rest or in transit • Force strong password policies • Enable logging of security events • Notify end users of security events.
Insecure Cloud Interface Related to the cloud interface used to interact with the IoT device. Typically this would imply poor authentication controls or data traveling in an unencrypted format allowing an attacker access to the device or the underlying data	• Account Enumeration • No Account Lockout • Credentials Exposed in Network Traffic	Ensure following • At the first time setup, default usernames and password must be changed. • Password reset mechanisms should not be vulnerable. • There must be some mechanism to lockout account after few failed unauthorized access attempts • Cloud-based web interface is not susceptible to XSS, SQLi or CSRF • In wireless networks connection, IoT object must send their sensitive information in secure way. • Implement multi factor authentication.
Insecure Mobile Interface Similar to the Cloud Interface, weak authentication or unencrypted data channels can allow an attacker access to the device or underlying data of an IoT device that uses a vulnerable mobile interface for user interaction	• Account Enumeration • No Account Lockout • Credentials Exposed in Network Traffic	Ensure following • At the first time setup, default usernames and password must be changed. • Password reset mechanisms should not be vulnerable. • There must be some mechanism to lockout account after few failed unauthorized access attempts • In wireless networks connection, IoT object must send their sensitive information in secure way. • Implement multi factor authentication.

REFERENCES

Abdul-Ghani, H. A., & Konstantas, D. (2019). A Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective. *Journal of Sensor and Actuator Networks*, *8*(2), 22. doi:10.3390/jsan8020022

Abdul-Ghani, H. A., Konstantas, D., & Mahyoub, M. (2018). A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. *International Journal of Advanced Computer Science and Applications*, *9*. doi:10.14569/IJACSA.2018.090349

Aggarwal, A., Chaubey, N., & Jani, K. A. (2013). A simulation study of malicious activities under various scenarios in Mobile Ad hoc Networks (MANETs). In Proceedings of the 2013 International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s) (pp. 827-834). IEEE.

Arias, O., Ly, K., & Jin, Y. (2017). Security and Privacy in IoT Era. In H. Yasuura, C.-M. Kyung, Y. Liu, & Y.-L. Lin (Eds.), *Smart Sensors at the IoT Frontier* (pp. 351–378). Cham: Springer International Publishing; doi:10.1007/978-3-319-55345-0_14

Arış, A., Oktuğ, S. F., & Voigt, T. (2018). Security of Internet of Things for a Reliable Internet of Services. In I. Ganchev, R. D. van der Mei, & H. van den Berg (Eds.), *Autonomous Control for a Reliable Internet of Services: Methods, Models, Approaches, Techniques, Algorithms, and Tools* (pp. 337–370). Cham: Springer International Publishing; doi:10.1007/978-3-319-90415-3_13

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. doi:10.1016/j.comnet.2010.05.010

Chandrashekhar, K. (2016, September 19). *Internet of Things (IoT) Characteristics*. Retrieved from [REMOVED HYPERLINK FIELD]https://www.linkedin.com/pulse/internet-things-iot-characteristics-kavyashree-g-c

Chaubey, N., Aggarwal, A., Gandhi, S., & Jani, K. A. (2015). Performance analysis of TSDRP and AODV routing protocol under black hole attacks in manets by varying network size. In *Proceedings of the 2015 Fifth International Conference on Advanced Computing & Communication Technologies* (pp. 320-324). IEEE. 10.1109/ACCT.2015.62

Chaubey, N., Akshai Aggarwal, S. G., & Jani, K. A. (2015). Effect of pause time on AODV and TSDRP routing protocols under black hole attack and DoS attacks in MANETs. In *Proceedings of the 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 1807-1812). IEEE.

Chaubey, N. K. (2016). Security analysis of vehicular ad hoc networks (VANETs): A comprehensive study. *International Journal of Security and Its Applications*, *10*(5), 261–274. doi:10.14257/ijsia.2016.10.5.25

Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., & Jin, Y. (2018). Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice. *Journal of Hardware and Systems Security*, *2*(2), 97–110. doi:10.100741635-017-0029-7

Cisco. (2014). The Internet of Things Reference Model. In *Proceedings of the Internet of Things World Forum*. Academic Press.

Dorai, R. K. V. (2011). SQL injection—database attack revolution and prevention. *J. Int. Commercial Law Technol.*, *6*, 224.

Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security analysis of emerging smart home applications. In *Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP)* (pp. 636-654). IEEE. doi:10.1109/SP.2016.44

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. doi:10.1016/j.future.2013.01.010

Ishino, M., Koizumi, Y., & Hasegawa, T. (2014). A Study on a Routing-Based Mobility Management Architecture for IoT Devices. In *Proceedings of the 2014 IEEE 22nd International Conference on Network Protocols* (pp. 498-500). doi:10.1109/ICNP.2014.78

Kumar, J. S., & Patel, D. R. (2014). A Survey on Internet of Things: Security and Privacy Issues. *International Journal of Computers and Applications*, *90*, 20–26. doi:10.5120/15579-4304

Lee, H. (2016). *IoT: Architecture*. Juxtology. Retrieved from https://juxtology.com/iot-transformation/iot-world-forum/

Lin, H., & W. Bergmann, N. (2016). IoT Privacy and Security Challenges for Smart Home Environments. *Information, 7*, 44. doi:10.3390/info7030044

Masoodi, F., Alam, S., Siddiqui, S., & Liz, L. (2019). 3). Security & Privacy Threats, Attacks and Countermeasures in Internet of Things. *International Journal of Network Security & Its Applications*, *11*(02), 67–77. doi:10.5121/ijnsa.2019.11205

Mosenia, A., & Jha, N. K. (2017). A Comprehensive Study of Security of Internet-of-Things. *IEEE Transactions on Emerging Topics in Computing*, *5*(4), 586–602. doi:10.1109/TETC.2016.2606384

Pal, A. (n.d.). *The Internet of Things (IoT) – Threats and Countermeasures*. CSO. Retrieved from [REMOVED HYPERLINK FIELD]https://www.cso.com.au/article/575407/internet-things-iot-threats-countermeasures/

Parno, B., Perrig, A., & Gligor, V. (2005). Distributed Detection of Node Replication Attacks in Sensor Networks. In *Proceedings of the 2005 IEEE Symposium on Security and Privacy* (pp. 49-63). IEEE Computer Society. 10.1109/SP.2005.8

Patel, M., Aggarwal, A., & Chaubey, N. (2017). Wormhole attacks and countermeasures in wireless sensor networks: A survey. *IACSIT International Journal of Engineering and Technology*, *9*(2), 1049–1060. doi:10.21817/ijet/2017/v9i2/170902126

Patel, M., Aggarwal, A., & Chaubey, N. (2018). Analysis of Wormhole Attacks in Wireless Sensor Networks. In *Recent Findings in Intelligent Computing Techniques* (pp. 33–42). Springer Singapore.

Patel, M., Aggarwal, A., & Chaubey, N. (2018). Variants of wormhole attacks and their impact in wireless sensor networks. In Progress in Computing, Analytics and Networking (pp. 637-642). Springer Singapore.

Postscapes. (n.d.). *Internet of Things Infographic*. Retrieved from [REMOVED HYPERLINK FIELD]https://www.postscapes.com/what-exactly-is-the-internet-of-things-infographic/

Tomić, I., & McCann, J. A. (2017). A survey of potential security issues in existing wireless sensor network protocols. *IEEE Internet of Things Journal*, *4*(6), 1910–1923. doi:10.1109/JIOT.2017.2749883

Wikipedia. (n.d.). Internet of things. Retrieved from https://en.wikipedia.org/wiki/Internet_of_Things