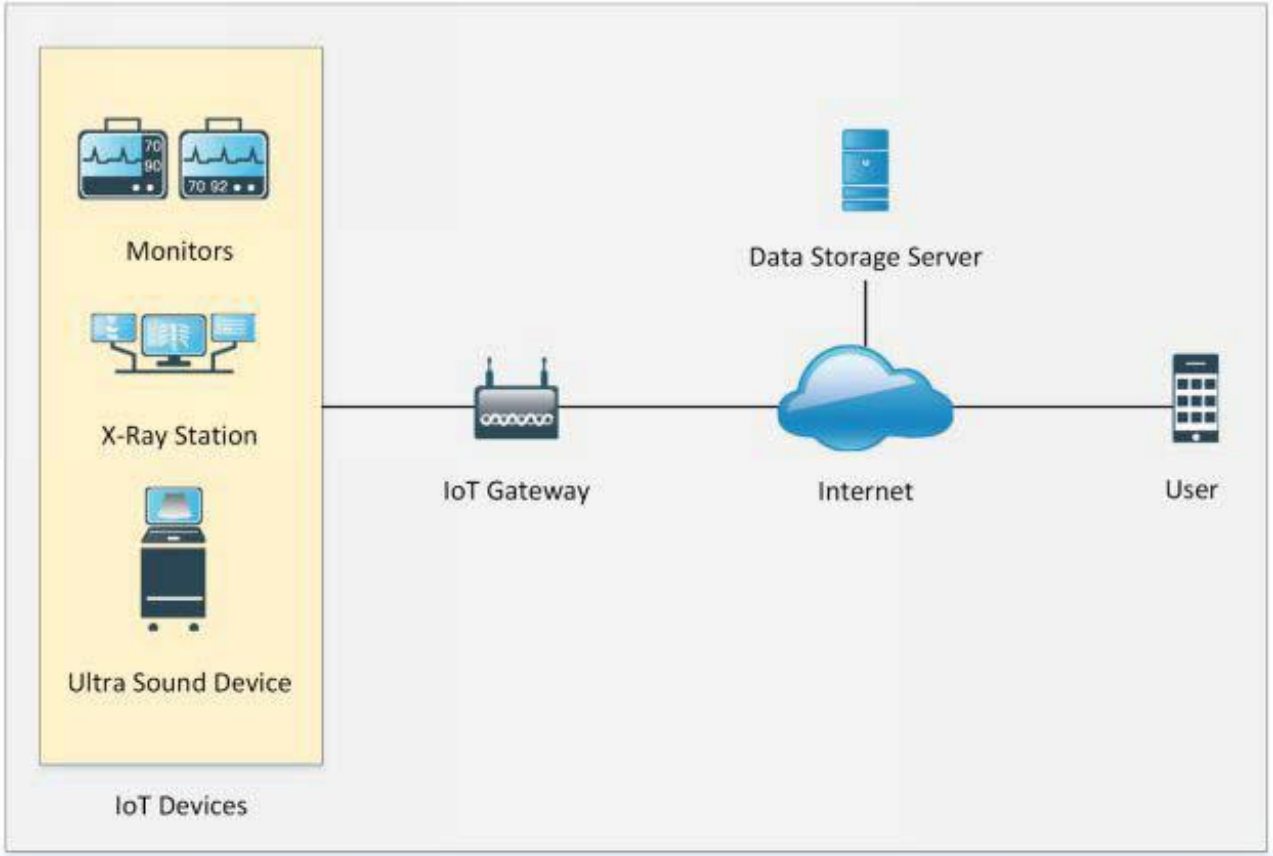
Introduction to IoT

The world is rapidly moving towards automation. the necessity for automated devices which controls our daily tasks on fingertips is increasing day by day. As we all know the performance and productivity difference between manual and automatic processes, moving towards interconnection of things will advance & make the method even faster. The term "Things" refers to the machines, appliances, sensors and lots of other devices.

How Does IoT Works

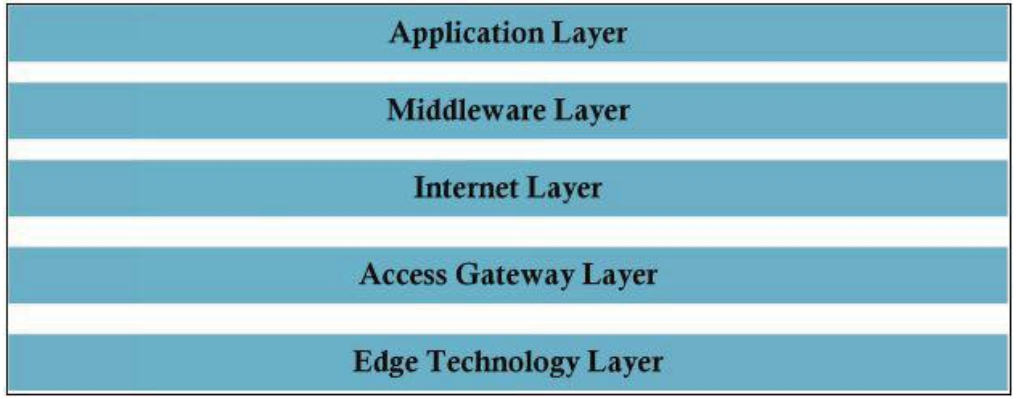
IoT devices may either use IoT gateways to speak with the web , or they could be directly communicating with the web . Integration of controlled equipment, logic controller & advanced programmable electronic circuits make them capable of communicating and being controlled remotely.



IoT Architecture

The architecture of IoT depends upon 5 layers which are as follows:

1. Application Layer
2. Middleware Layer
3. Internet Layer
4. Access Gateway Layer
5. Edge Technology Layer



- The Application layer is liable for delivering the info to the users at the appliance layer. this is often a interface to regulate , manage and command these IoT devices.
- Middleware Layer is for device and knowledge management.
- Internet Layer is liable for endpoints connectivity.
- Access Gateway Layer is liable for protocol translation and messaging.
- Edge Technology Layer covers IoT capable devices.

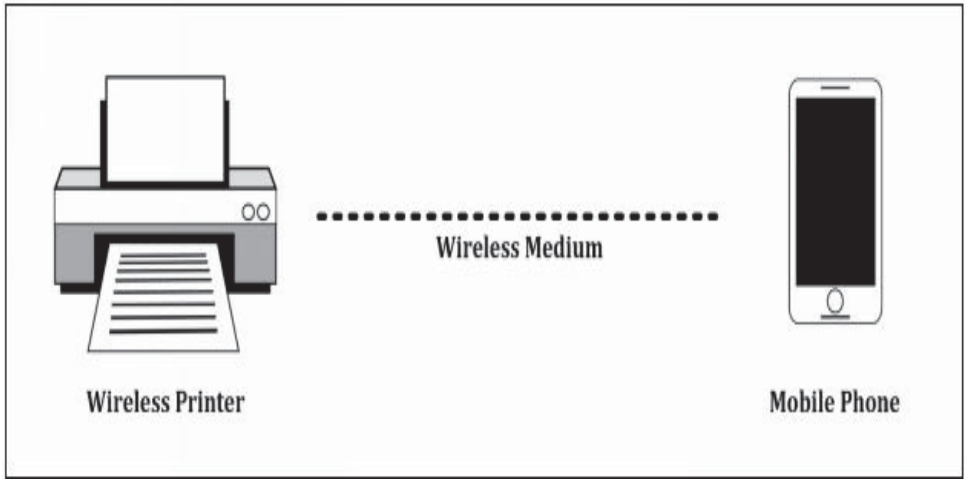
IoT Communication Models

There are several ways during which IoT devices can communicate with the opposite devices.

The following are a number of the IoT communication models.

Device to device model

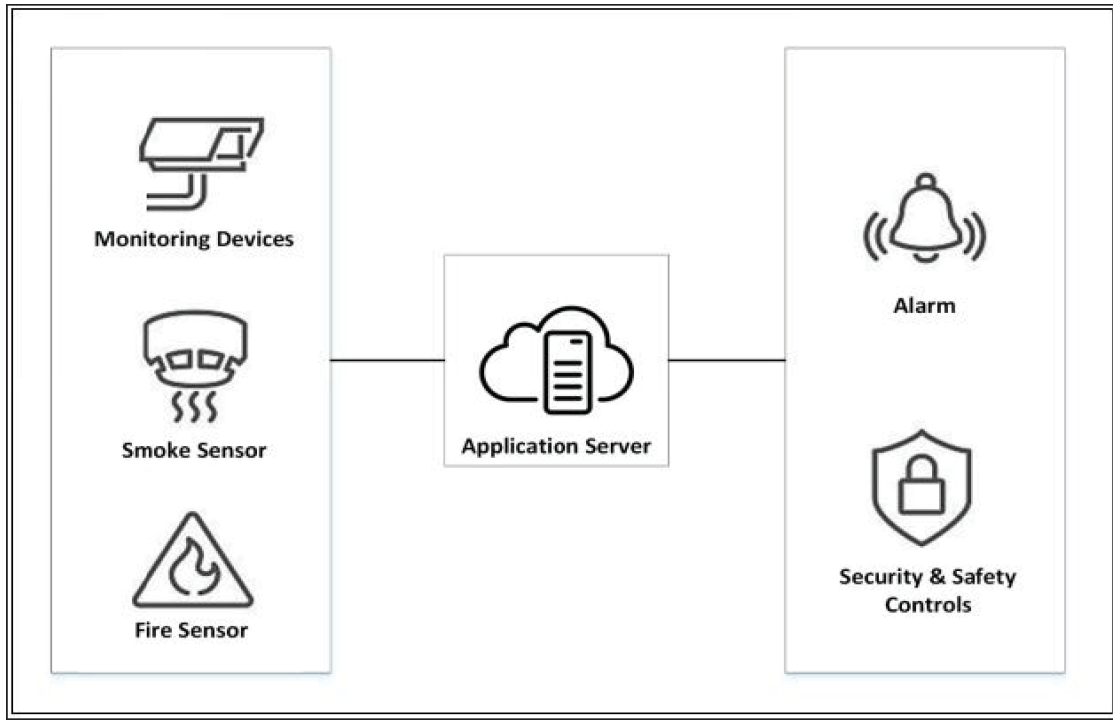
Device to device model could be a basic IoT communication model during which two devices are communicating with one another without interfering the other device. Communication between these two devices is established employing a communication medium like a wireless network. Any household appliance connected with wireless remote through a medium like Wi-Fi, Bluetooth, NFC or RFID are often an example of Device to Device communication model



IoT Communication Models

Device to Cloud model

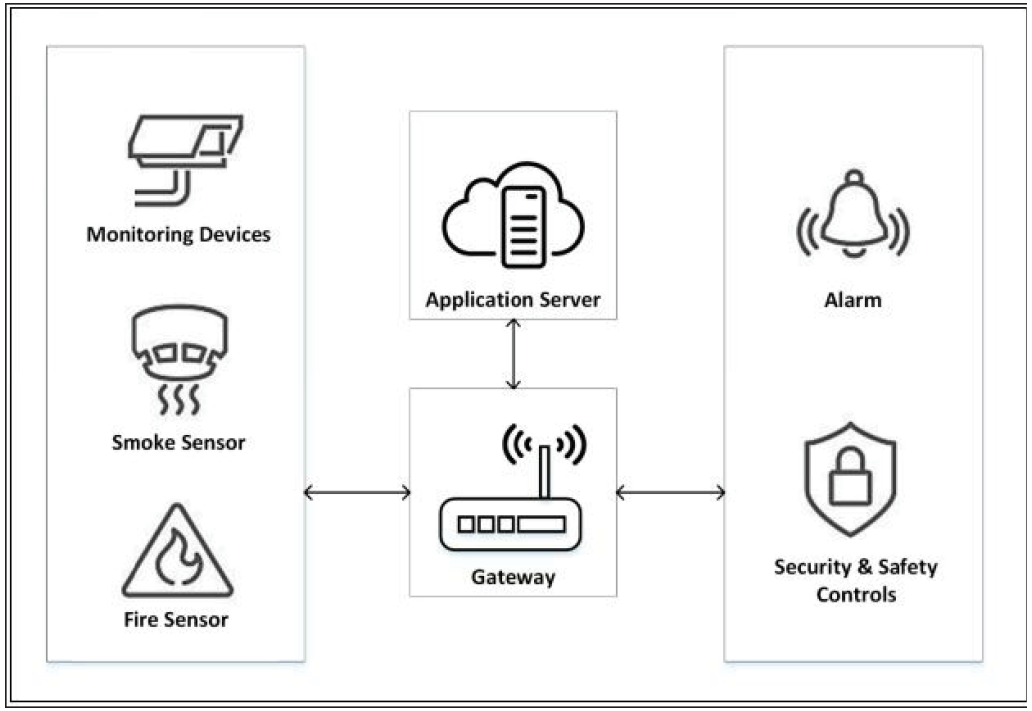
Device-to-Cloud Model is another model of IoT device communication during which IoT devices are directly communicating with the appliance server. Device-to-Cloud communication scenarios are found during a manufacturing environment where different sensors are communicating with the appliance server. Application severs process the info , and perform predictive maintenance, required and remediation actions to automate processes and accelerate production.



IoT Communication Models

Device to Gateway model

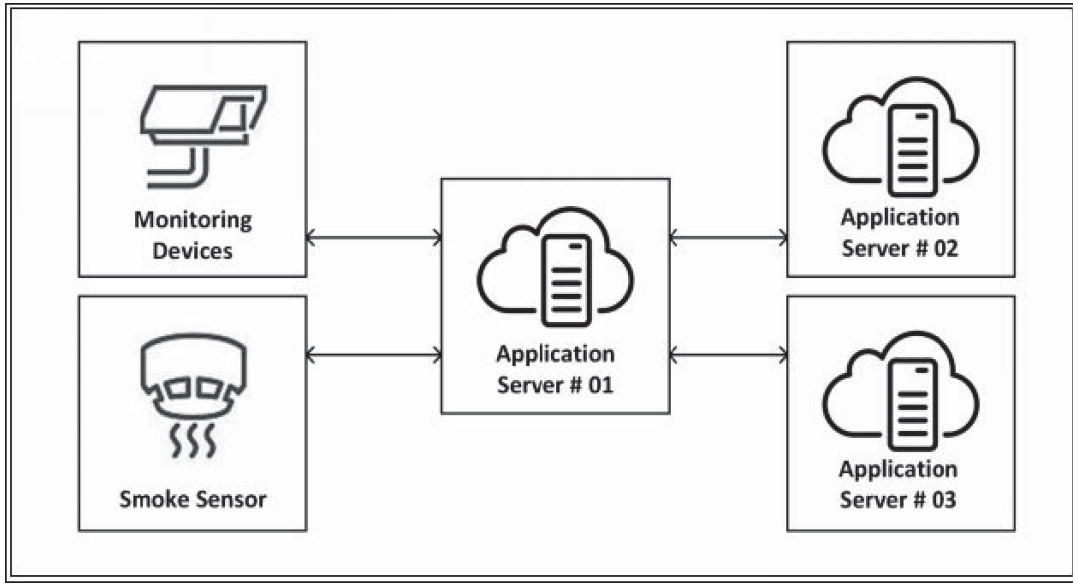
Device-to-Gateway model is analogous to Device to cloud model. IoT gateway device is added during this Device-to-Gateway model which collects the info from sensors and send it to the remote application server. additionally , you'll have a consolidation point where you'll inspect and control the info being transmitted.



IoT Communication Models

Back-End Data-Sharing Model

Back-End Data-Sharing Model is a complicated model during which devices are communicating with the appliance servers. This scenario is employed during a collective partnership between different application providers. Back-End Data Sharing model extends the Device-to- Cloud model to a scalable scenario where these sensors accessed and controlled by multiple authorized third-parties.



Understanding IoT Attacks

Challenges to IoT

There are many challenges to the web of Things (IoT) deployment. because it brings ease, mobility & more control over processes. There are threats, vulnerabilities, & challenges to IoT technology. Major challenges to IoT technology are as follows:

1. Difficult to update firmware and OS
2. Vulnerable Interfaces
3. Interoperability Issues
4. Lack of Vendor Support
5. Lack of Security
6. Physical Security Risk

IoT Attack Areas

Following are the most common attack areas for IoT network:

- Access Control.
- Firmware Extraction.
- Device memory containing credentials.
- Resetting to an insecure state.
- Removal of storage media.
- Privileges Escalation.
- Firmware Attacks.
- Network Services Attacks.
- Unencrypted Local Data Storage.
- Confidentiality and Integrity issues.
- Cloud Computing Attacks.
- Web Attacks.
- Malicious updates.
- Insecure APIs.
- Mobile Application threats.

IoT Attack

DDos Attack:

DDOS attack as defined earlier intended for creating services of the target unavailable. Using DDOS attack, all IoT devices, IoT gateways and application servers are often targeted, and flooding request towards them may result in DOS.

Rolling Code Attack:

Rolling code is another technique to take advantage of . during this technique, hacker capture the code, sequence from transmitter devices along side simultaneously blocking the receiver to receive the signal. This captured code will later use to realize unauthorized access.

BlueBorne Attack:

The blueborne attack is performed using many techniques to take advantage of Bluetooth vulnerabilities. This collection of techniques to realize unauthorized access to Bluetooth enabled devices are called a Blueborne attack.

IoT Attack

Jamming Attack:

Jamming of signals to stop devices to speak with one another & with the server

Backdoor:

Deploying a backdoor on a computer of an employee of a corporation , or victim to realize unauthorized access to the private network. it's not all about creating a backdoor on IoT devices.

Some other sorts of IoT attacks include:

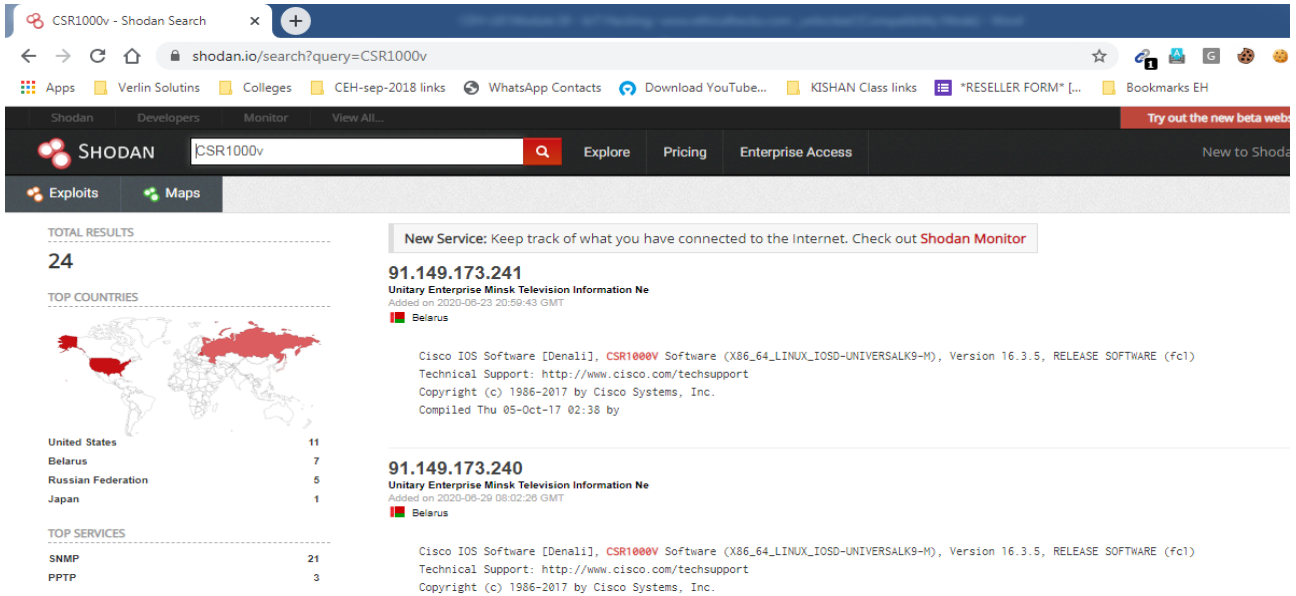
- Eavesdropping
- Ransomware Attack
- Exploit Kits
- Man-in-the-Middle Attack
- Side Channel Attack
- Replay Attack
- Sybil Attack
- Forged Malicious Devices

IoT Hacking Methodology

IoT Hacking methodology platform is same as a strategy for other platforms.

Information Gathering

The 1st step in hacking IoT environment requires operation . operation includes extraction of data like IP addressing, running protocols, open ports, sort of devices, vendor's information, etc. Shodan, Censys, and Thingful are the program to seek out out information about IoT devices. Shodan may be a helpful platform for locating and gathering information about IoT devices. As shown within the figure on subsequent page, information can look for Webcams deployed across the globe.



IoT Hacking Methodology

Vulnerability Scanning

Vulnerability scanning involves scanning the network and devices for identification of vulnerabilities like weak passwords, software & firmware bugs, default configuration,Multi-ping, Nmap, Vulnerability scanner, Foren6 are used for scanning against vulnerabilities.

Launch Attack

Launching attack phase includes exploiting these vulnerabilities using different attacks such as DDoS, Rolling Code attack, jamming, etc. RFCrack and Attify Zigbee Framework, HackRF are popular tools for attacking.

Gain Access

Gaining access involves taking control over IoT environment. Gaining access, escalating privileges to administrator, installation of backdoor also are included during this phase

Maintain Attack

Maintaining attack involves logging out without being detected, clearing logs and covering tracks.

IoT Hacking Countermeasures

Countermeasure for IoT devices includes the subsequent measures which are recommended by the manufacturing companies.

- User account lockout
- Firmware update
- Disable Telnet
- Use encrypted communication such as SSL/TLS
- Use strong password
- Use encryption of drives
- Periodic assessment of devices
- Secure password recovery
- Two-Factor Authentication
- Disable UPnP
- Block unnecessary ports