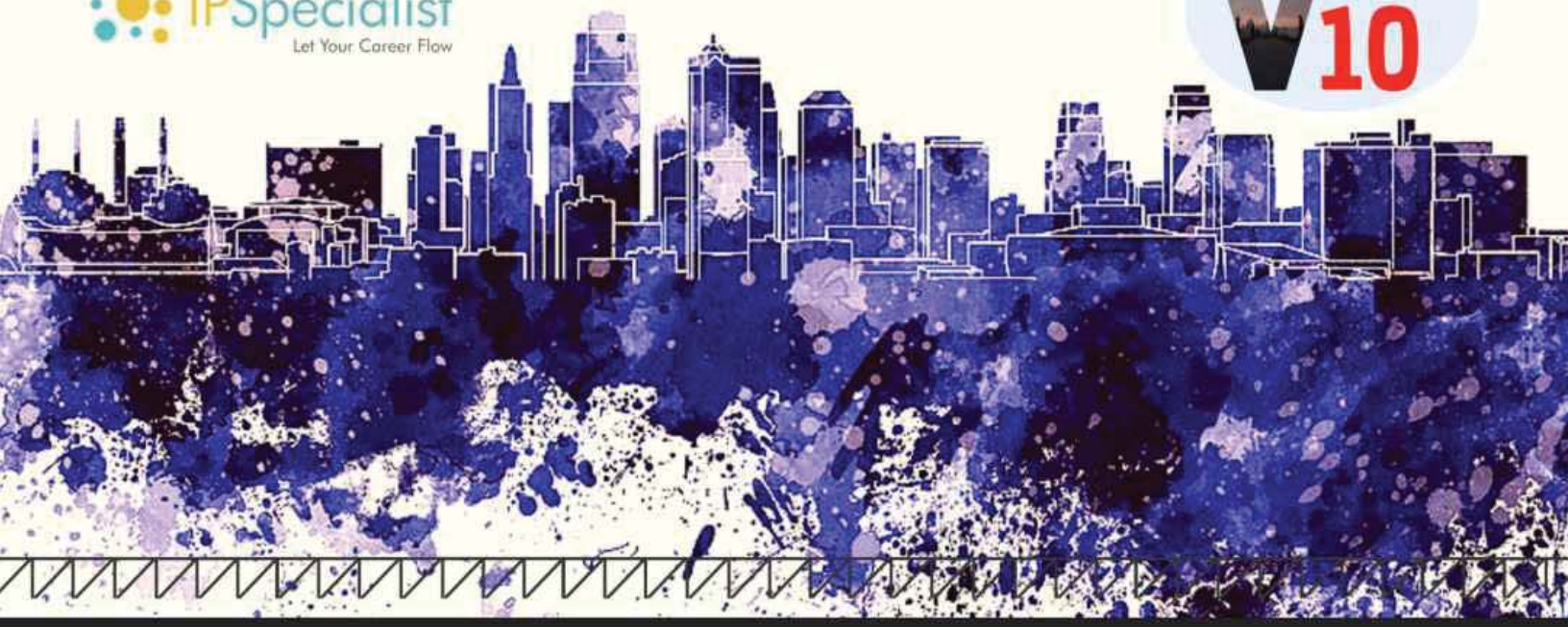
IPSpecialist
Let Your Career Flow

V10



CEH V10 EC-COUNCIL CERTIFIED ETHICAL HACKER

MOST DEMANDING COMPLETE HACKING GUIDE

EXAM: 312-50

C|EH
Certified Ethical Hacker

"To beat a hacker, you need to think like a hacker

MOST ADVANCED HACKING COURSE

www.ipspecialist.net

Chapter 18: IoT Hacking

Technology Brief

This module is added in CEHv10 with the objectives of understanding IoT concepts, an overview of IoT threats and attacks, IoT hacking methodology, tools and techniques of IoT hacking, security tool and penetration testing. Internet of Things (IoT) is an environment of physical devices such as home appliances, electronic devices, sensors, etc. which are embedded with software programs and network interface cards to make them capable of connecting and communicating with the network.

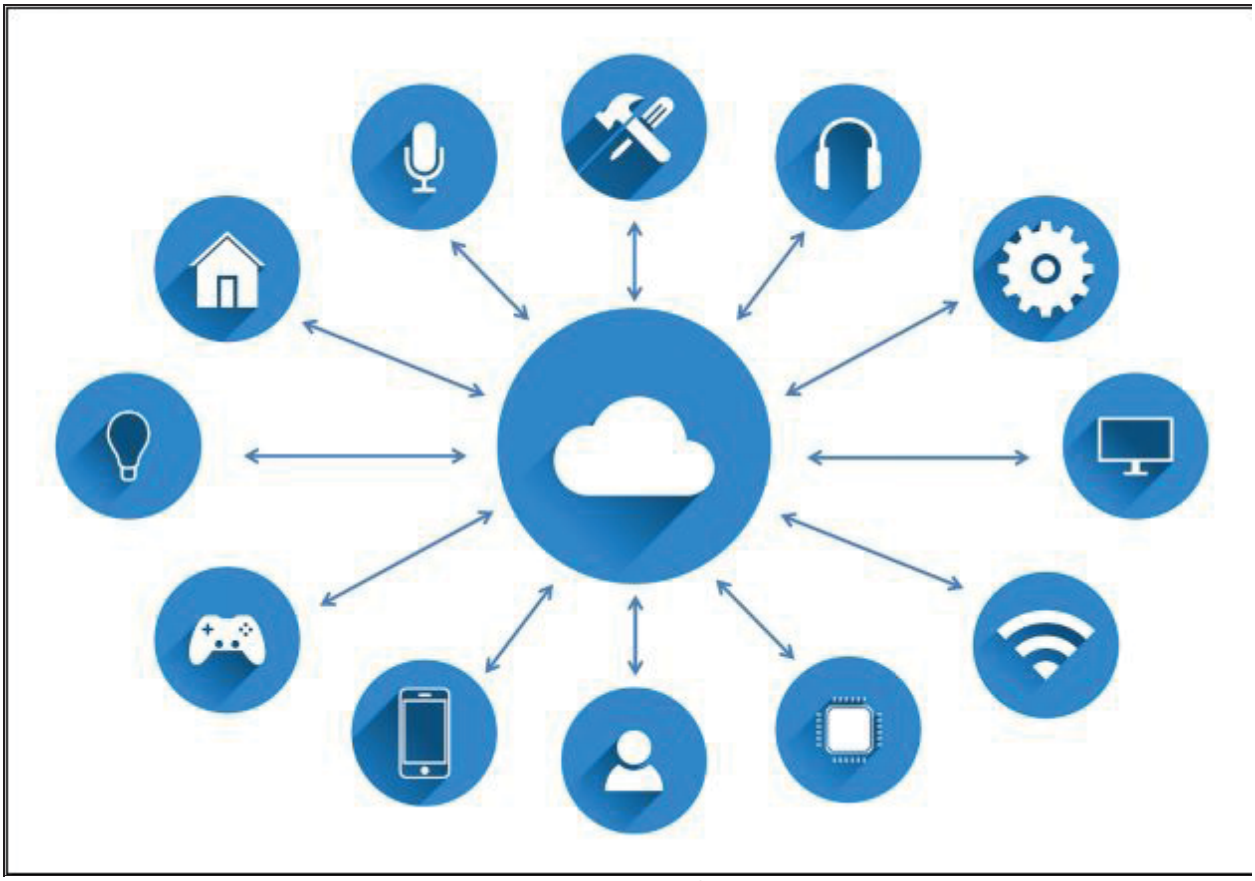


Figure 18-01: Internet of Things (IoT)

Internet of Things (IoT) Concept

The world is rapidly moving towards automation. The need for automated devices which controls our daily tasks on fingertips is increasing day by day. As we know the performance and productivity difference between manual and automated processes, moving towards interconnection of things will advance and make the process even faster. The term "Things" refers to the machines, appliances, vehicles, sensors and many other devices. An example of this automation process through the Internet of Things is connecting a CCTV camera placed in a building captures intrusion and immediately generate alerts on client devices at the remote location. Similarly, we can connect other devices over the internet to communicate with other devices.

IoT technology requires unique identity. Unique identity refers to the IP address, especially IPv6 addresses to provide each and every device a unique identity. IPv4 and IPv6 planning and deployment over an advance network structure requires thorough consideration of advanced strategies and techniques. In IP version 4, a 32-bit address is assigned to each network node for the identification while in IP version 6, 128 bits are assigned to each node for unique identification. IPv6 is an advanced version of IPv4 that can accommodate the emerging popularity of the internet, increasing number of users, and a number of devices and advancements in networking. Advance IP address must consider IP address which supports efficiency, reliability, and scalability in the overall network model.

How does the Internet of Things works?

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

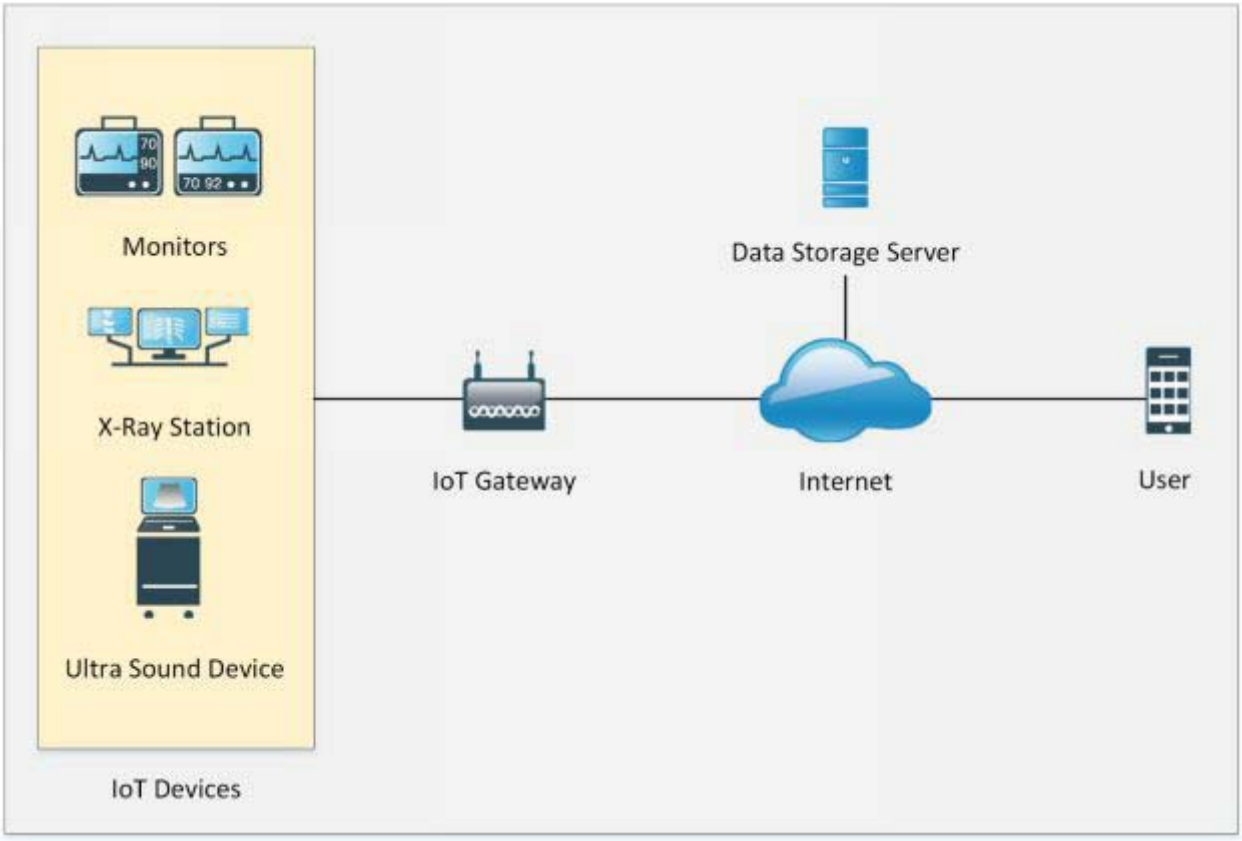


Figure 18-02: Working of the Internet of Things (IoT)

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

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

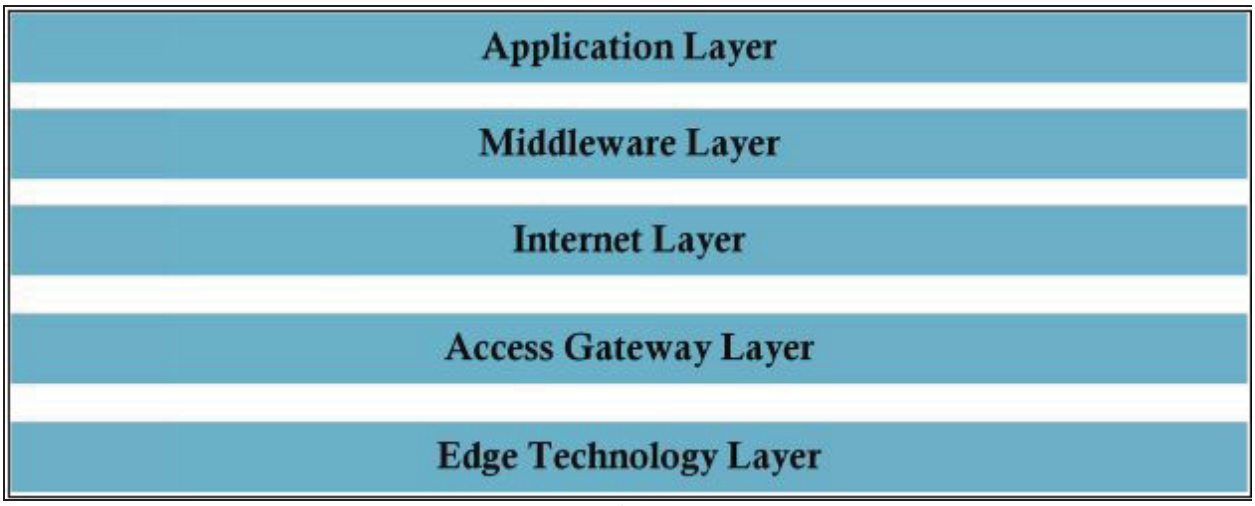


Figure 18-03: Internet of Things (IoT) Architecture

- The Application layer is responsible for delivering the data to the users at the application layer. This is a user interface to control, manage and command these IoT devices.
- Middleware Layer is for device and information management.
- Internet Layer is responsible for endpoints connectivity.
- Access Gateway Layer is responsible for protocol translation and messaging.
- Edge Technology Layer covers IoT capable devices.

IoT Technologies and Protocols				
Wireless Communication			Wired Communication	Operating System
Short Range	Medium Range	Long Range		
Bluetooth Low Energy (BLE)	Ha-Low	Low-Power Wide Area Networking (LPWAN)	Ethernet	RIOT OS
Light-Fidelity (Li-Fi)	LTE-Advanced	Very Small Aperture Terminal (VSAT)	Multimedia over Coax Alliance (MoCA)	ARM mbed OS
Near Field Communication		Cellular	Power-Line Communication	Real Sense OS X

(NFC)			(PLC)	
Radio Frequency Identification (RFID)				Ubuntu Core
Wi-Fi				Integrity RTOS

Table 18-01: Internet of Things (IoT) Technologies and Protocols

IoT Communication Models

There are several ways in which IoT devices can communicate with the other devices. The following are some of the IoT communication models.

Device-to-Device Model

Device to device model is a basic IoT communication model in which two devices are communicating with each other without interfering any other device. Communication between these two devices is established using a communication medium such as a wireless network. An example of Device-to-Device communication model can be a Mobile phone user and a Wi-Fi printer. The user can connect Wi-Fi printer using Wi-Fi connection and send commands to print. These devices are independent of vendor. The mobile phone of a vendor can communicate with the wireless printer of different manufacture because of interoperability. Similarly, any home appliance connected with wireless remote control through a medium such as Wi-Fi, Bluetooth, NFC or RFID can be an example of Device to Device communication model.

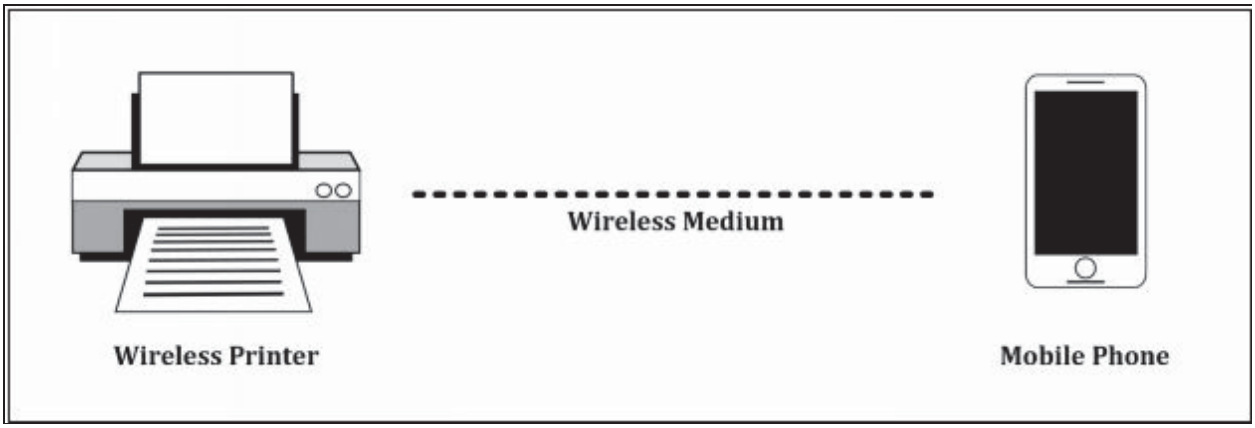


Figure 18-04: Device-to-Device Communication Model

Device-to-Cloud Model

Device-to-Cloud Model is another model of IoT device communication in which IoT devices are directly communicating with the application server. For example, consider a real-life scenario of a home where multiple sensors are installed for security reasons such as motion detector, cameras, temperature sensor, etc. These sensors are directly connected to the application server which can be hosted locally or on a cloud. The application server will provide information exchange between these devices.

Similarly, Device-to-Cloud communication scenarios are found in a manufacturing environment where different sensors are communicating with the application server. Application severs process the data, and perform predictive maintenance, required and remediation actions to automate processes and accelerate production.

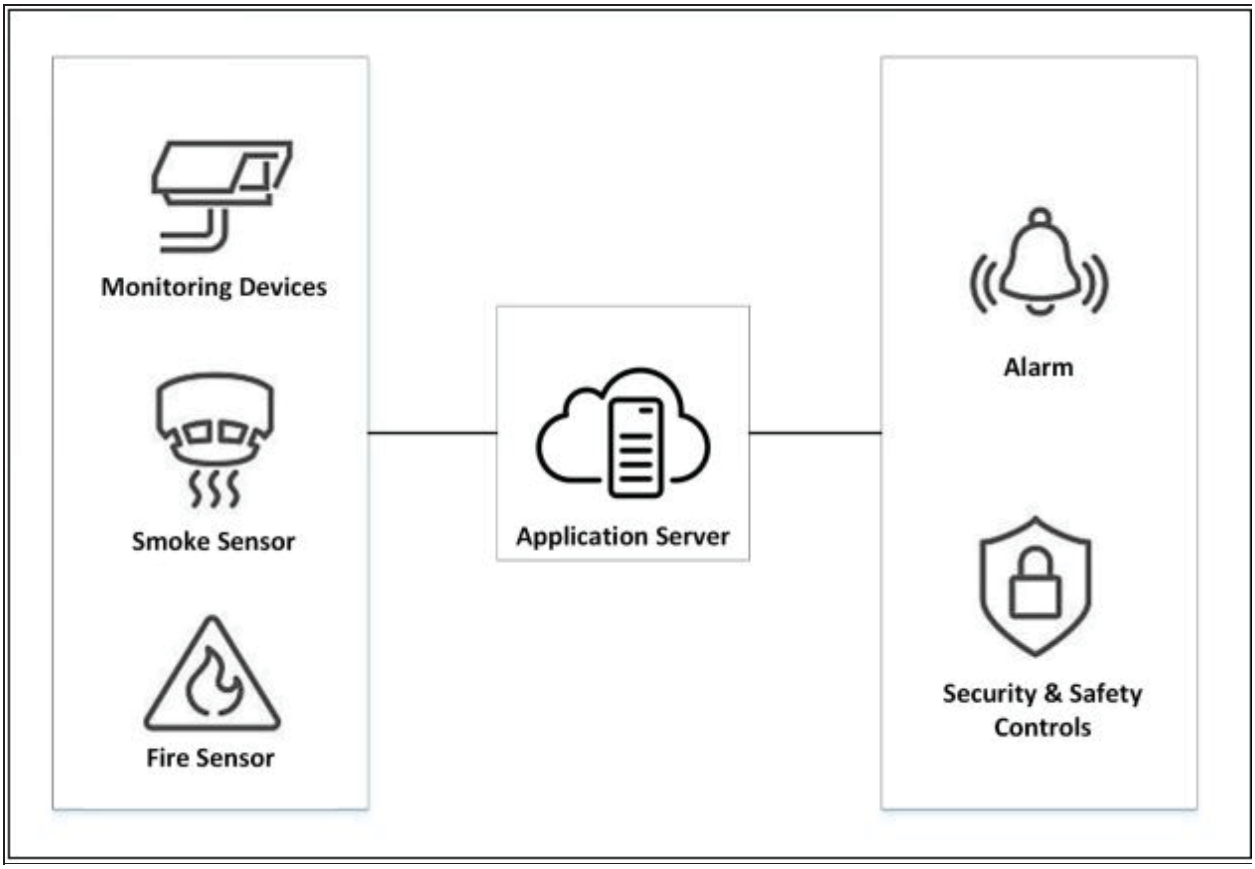


Figure 18-05: Device-to-Cloud Communication Model

Device-to-Gateway Model

Device-to-Gateway model is similar to Device to cloud model. IoT gateway device is added in this Device-to-Gateway model which collects the data from sensors and send it to the remote application server. In addition, you

will have a consolidation point where you can inspect and control the data being transmitted. This gateway could provide security and other functionality such as data or protocol translation.

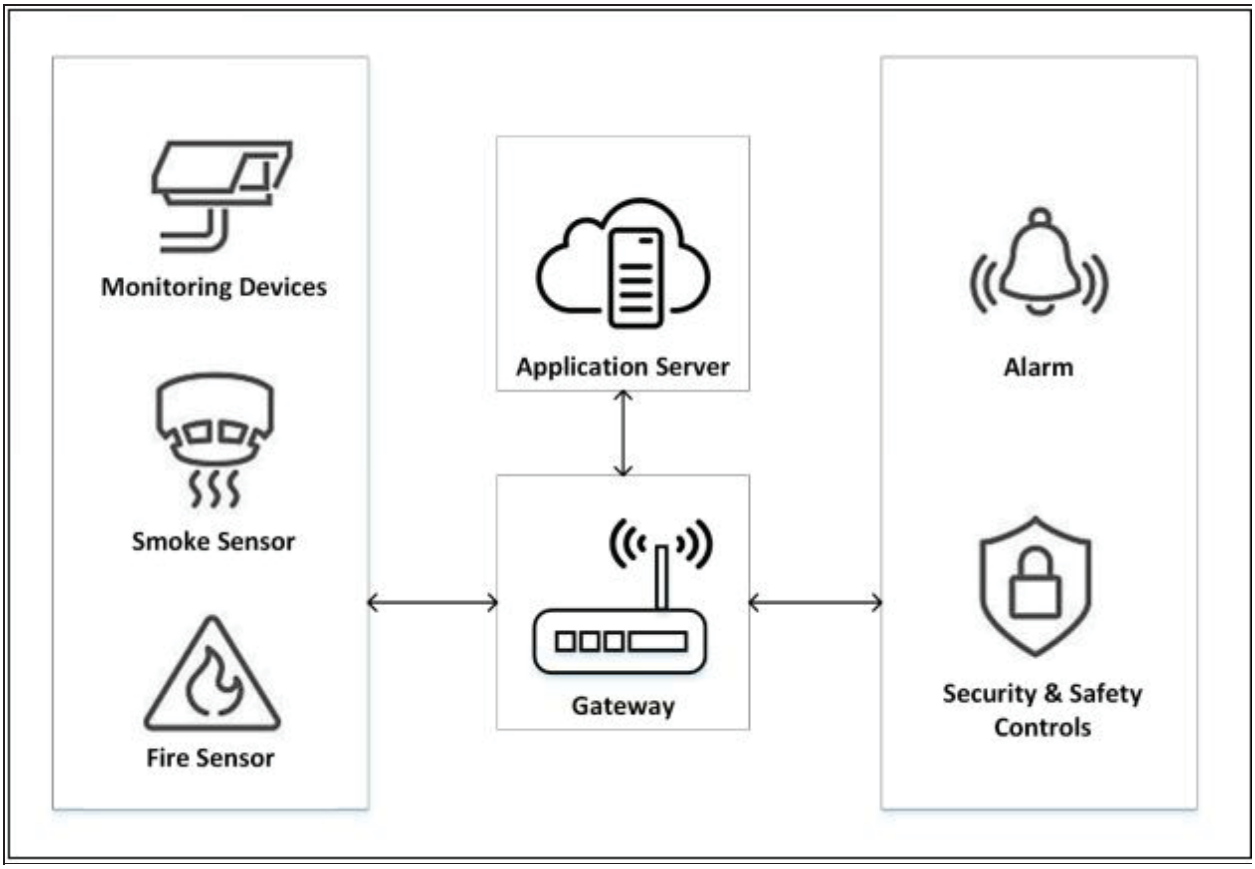


Figure 18-06: Device-to-Gateway Communication Model

Back-End Data-Sharing Model

Back-End Data-Sharing Model is an advanced model in which devices are communicating with the application servers. This scenario is used in 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 are accessed and controlled by multiple authorized third-parties.

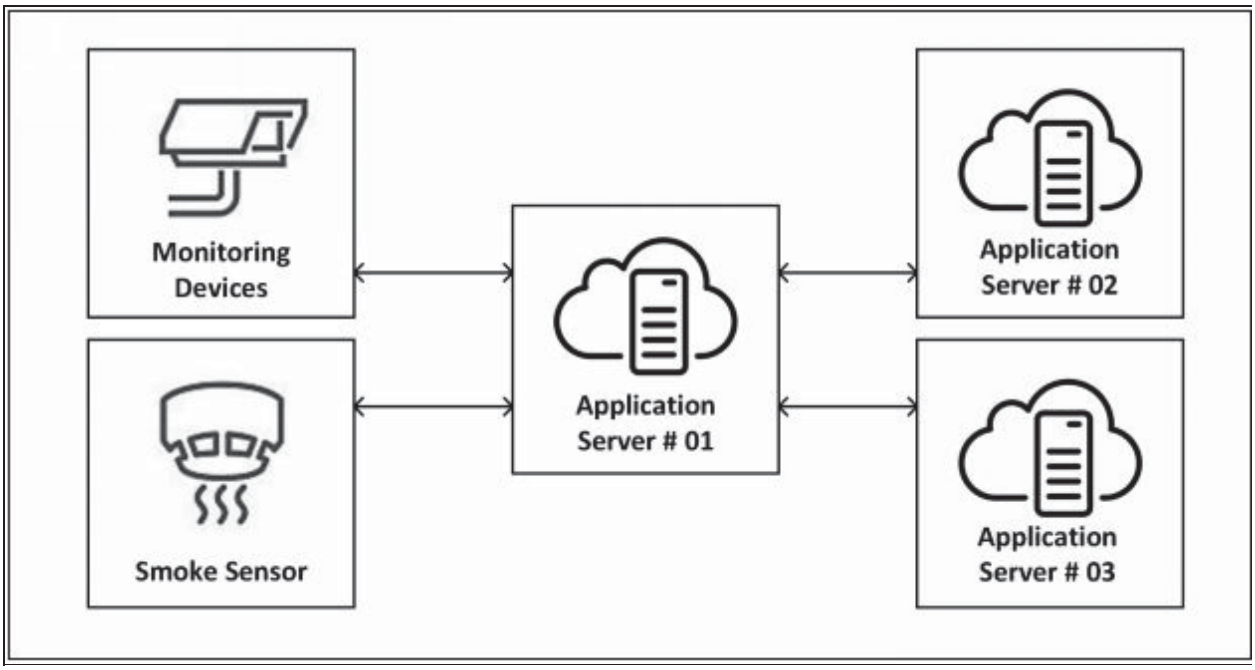


Figure 18-07: Back-End Data Sharing Model

Understanding IoT Attacks

Challenges to IoT

There are many challenges to the Internet of Things (IoT) deployment. As it brings ease and mobility and more control over processes. There are threats, vulnerabilities, and challenges to IoT technology. Some major challenges to IoT technology are as follows:

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

OWASP Top 10 IoT Vulnerabilities

The OWASP Top 10 IoT Vulnerabilities from 2014 are as follows:

Rank	Vulnerabilities
I1	Insecure Web Interface
I2	Insufficient Authentication/Authorization
I3	Insecure Network Services
I4	Lack of Transport Encryption/Integrity Verification
I5	Privacy Concerns
I6	Insecure Cloud Interface
I7	Insecure Mobile Interface
I8	Insufficient Security Configurability
I9	Insecure Software/Firmware
I10	Poor Physical Security

Table 18-02: OWASP Top 10 IoT Vulnerabilities

IoT Attack Areas

The following are the most common attack areas for IoT network:

- Device memory containing credentials.
- Access Control.
- Firmware Extraction.
- Privileges Escalation.

- Resetting to an insecure state.
- Removal of storage media.
- Web Attacks.
- Firmware Attacks.
- Network Services Attacks.
- Unencrypted Local Data Storage.
- Confidentiality and Integrity issues.
- Cloud Computing Attacks.
- Malicious updates.
- Insecure APIs.
- Mobile Application threats.

IoT Attacks

DDoS Attack

Distributed-Denial of Service attack as defined earlier intended for making services of the target unavailable. Using Distributed-DOS attack, all IoT devices, IoT gateways and application servers can be targeted, and flooding request towards them can result in denial of service.

Rolling Code Attack

Rolling code or Code hopping is another technique to exploit. In this technique, attacker capture the code, sequence or signal coming from transmitter devices along with simultaneously blocking the receiver to receive the signal. This captured code will later use to gain unauthorized access.

For example, a victim sends a signal to unlock his garage or his car. Central locking of cars works on radio signaling. An attacker using a signal jammer, prevent the car's receiver to receive the signal and simultaneously capture the signal sent by the owner of the car. Later, an attacker can unlock the car using captured signal.

BlueBorne Attack

The blueborne attack is performed using different techniques to exploit Bluetooth vulnerabilities. This collection of techniques to gain unauthorized access to Bluetooth enabled devices are called a Blueborne attack.

Jamming Attack

Jamming of signals to prevent devices to communicate with each other and

with the server.

Backdoor

Deploying a backdoor on a computer of an employee of an organization, or victim to gain unauthorized access to the private network. It is not all about creating a backdoor on IoT devices.

Some other types of IoT attacks include:

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

IoT Hacking Methodology

Hacking methodology for IoT platform is same as a methodology for other platforms. Methodology for IoT hacking is defined below:

Information Gathering

The first step in hacking IoT environment requires information gathering. Information gathering includes extraction of information such as IP addressing, running protocols, open ports, type of devices, vendor's information, etc. Shodan, Censys, and Thingful are the search engine to find out information about IoT devices. Shodan is a helpful platform for discovering and gathering information about IoT devices. As shown in the figure on the next page, information can search for Webcams deployed across the world.

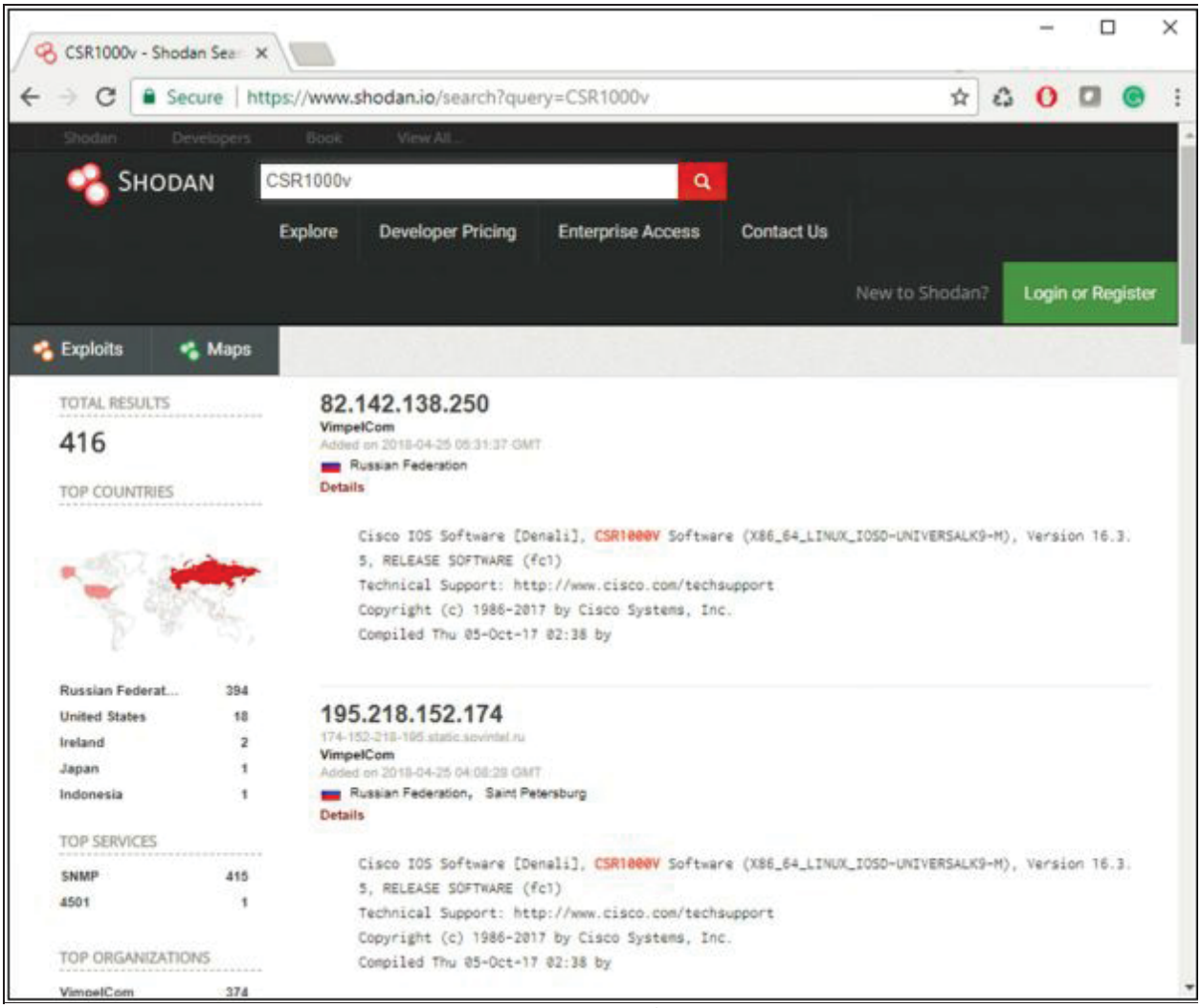


Figure 18-08: Shodan IoT Information Gathering

Vulnerability Scanning

Vulnerability scanning includes scanning the network and devices for identification of vulnerabilities such as weak passwords, software and firmware bugs, default configuration, etc. Multi-ping, Nmap, RIoT Vulnerability scanner, Foren6 are used for scanning against vulnerabilities.

Launch Attack

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

Gain Access

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

Maintain Attack

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

Countermeasures:

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

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