INTERNET OF THINGS DEVICES (IOT DEVICES)

Yusupov Jasurbek Shuxrat o'g'li[1] Parthasarathi Murugesan[2] Esther Magthalene Anne[3]

1. Master of MScIT , 2. Assoc. Professor & Dean- BS, 3. Asst. Professor-IT, Sambhram University Jizzakh - Uzbekistan @gmail.com 2. parthasarathi.murugesan@gmail.com 3. esthermathews22@gmail.com

Abstract: *Internet of things (IoT) devices are nonstandard computing hardware -- such as sensors, actuators or appliances -- that connect wirelessly to a network and can transmit data. IoT and IoT devices aid in making daily activities faster, easier or more convenient for consumers while also providing real-time data for industrial or enterprise use cases.*

Keywords: *Ultimate IoT implementation guide for businesses,IoT trends to keep an eye on in 2024, AI and IoT: How do the internet of things and AI work together?*

Introduction

IoT extends internet connectivity beyond typical computing devices -- such as desktops, laptops, smartphones and tablets -- to any range of traditionally dumb or non-internet-enabled physical devices and everyday objects. Embedded with technology, these devices can communicate and interact over the internet, and can be remotely monitored and controlled.

IoT devices have both industrial and consumer uses and are typically integrated into other tools such as mobile devices, industrial equipment and medical devices. Over a broad range, they can also be used in smart cities. They're then used to send data or interact with other IoT devices over a network.

What is an example of an IoT device?

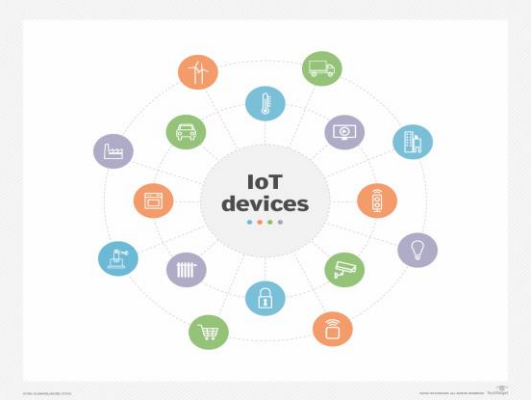
Connected devices are part of an ecosystem in which every device talks to other related devices in the environment to automate home and industry tasks. They can transmit sensor data to users, businesses and other intended parties. The devices can be categorized into three main groups: consumer, enterprise and industrial.

Consumer-connected devices include smart TVs, smart speakers such as Google Home, toys, wearables and smart appliances. In a smart home, for example, IoT devices are designed to sense and respond to a person's presence. When a person arrives home, their car communicates with the garage to open

the door. Once inside, the thermostat is already adjusted to a preset temperature, and the lighting is set to a lower intensity and color. Other smart home devices include sprinklers that adjust the amount of water distributed on the lawn based on the weather forecast and robotic vacuum cleaners that learn which areas of the home must be cleaned most often.

Enterprise IoT devices are edge devices designed for businesses. There are a wide variety of enterprise IoT devices available. These devices vary in capabilities but tend to be geared toward maintaining a facility or improving operational efficiency. Some options include smart locks, smart thermostats, smart lighting and smart security. Consumer versions of these technologies exist as well.

In the enterprise, smart devices can help with meetings. Smart sensors located in a conference room can help an employee locate and schedule an available room for a meeting, ensuring the proper room type, size and features are available.



Examples of IoT devices.

Consumer, enterprise and industrial IoT devices include smart TVs and smart sensors outfitted for conference rooms and assembly line machines.

Likewise, retailers can use RFID tags to track a business's goods, increasing inventory accuracy. Expanding on this idea, IoT devices are also used to keep track of inventory as it moves along in the supply chain for supply chain management.

Industrial IoT (IIoT) devices are designed for use in factories or other industrial environments. Most IIoT devices are sensors used to monitor an assembly line or other manufacturing processes. Sensor data is transmitted to monitor applications to ensure key processes are running optimally. These same sensors can also prevent unexpected downtime by predicting when parts need to be replaced.

If a problem occurs, the system can send a notification to a service technician informing them of what's wrong and what parts they need to fix the problem. This can save the technician from coming on site to diagnose the problem and then having to travel to a warehouse to get the part needed to fix the problem.

In the medical industry, IoT devices are used to monitor a patient's health and track their vitals. If a patient needs attention, these monitors send notifications to the relevant healthcare workers.

How do IoT devices work?

IoT devices vary in terms of functionality, but also have some similarities in how they work. First, IoT devices are physical objects designed to interact with the real world in some way. The device might be a sensor on an assembly line or an intelligent security camera. In either case, the device senses what's happening in its surrounding environment.

The devices themselves typically include an integrated CPU, firmware and a network adapter. In most cases, IoT devices connect to a Dynamic Host Configuration Protocol server and acquire an IP address that it can use to function on the network. Some IoT devices are directly accessible over the public internet, but most are designed to operate exclusively on private networks.

Although not an absolute requirement, many IoT devices are configured and managed through a software application. Some devices, however, have integrated web servers, eliminating the need for an external application.

Once an IoT device has been configured and begins to operate, most of its traffic is outbound. A security camera, for example, streams video data. Likewise, an industrial sensor streams sensor data. Some IoT devices such as smart lights, however, do accept inputs.

What is IoT device management?

Several challenges can hinder the successful deployment of an IoT system and its connected devices, including security, interoperability, power and processing capabilities, scalability and availability. Many of these problems can be addressed with IoT device management, either by adopting standard protocols or using services offered by a vendor.

Device management helps companies integrate, organize, monitor and remotely manage internet-enabled devices at scale, offering features critical to maintaining the health, connectivity and security of the IoT devices along their entire lifecycles.

IoT device management contains separate categories, including onboarding devices, configuration, maintenance, diagnostics and end-of-life management. Device management typically follows a pattern such as the following:

- Registration and activation.
- Authentication and authorization.
- Configuration.
- Provisioning.
- Monitoring and diagnostics.
- Troubleshooting.
- Firmware updates.

Some examples of standardized device management protocols include the Open Mobile Alliance device management and Lightweight Machine to Machine.

IoT device management services and software are also available from vendors, including Amazon, General Electric, Google, IBM and Microsoft.

IoT device connectivity and networking

The networking, communication and connectivity protocols used with internet-enabled devices largely depend on the specific IoT application deployed. Just as there are many different IoT applications, there are many different connectivity and communication options, including the following:

- Constrained Application Protocol, or CoAP.
- Datagram Transport Layer Security, or DTLS.
- MQ Telemetry Transport, or MQTT.
- Data Distribution Service, or DDS.
- Advanced Message Queuing Protocol, or AMQP.

Wireless protocols include the following:

- IPv6.
- Zigbee Bluetooth Low Energy.
- Z-Wave.
- Cellular, satellite, Wi-Fi and Ethernet can also be used.

Connectivity options have tradeoffs in terms of power consumption, range and bandwidth, all of which must be considered when choosing connected devices and protocols for an IoT application. These options range from high range, power consumption and bandwidth to low range, power consumption and bandwidth to high range, but low power consumption and bandwidth.

In most cases, IoT devices connect to an IoT gateway or another edge device where data can either be analyzed locally or sent to the cloud for analysis. Some devices have integrated data processing capabilities that minimize the amount of data that must be sent to the cloud or to the data center. This type of processing, which often uses machine learning capabilities that are integrated into the device, is becoming increasingly popular as IoT devices create more data.

What security risks do IoT devices pose?

The interconnection of traditionally dumb devices raises several questions in relation to security and privacy. As is often the case, IoT technology has moved more quickly than the mechanisms available to safeguard devices and their users.

Some of the top IoT security risks that organizations should address include the following:

- Increased attack surfaces.
- Unsecured hardware.
- Poor asset management.
- Shadow IoT.
- Unencrypted data transmissions.
- Domain name system (DNS) threats.
- Malicious node injections.
- IoT ransomware attacks.
- Firmware exploits.

One of the largest demonstrated remote hacks on IoT-connected devices occurred in October 2016. A distributed denial-of-service attack dubbed the Mirai botnet affected DNS on the east coast of the U.S, disrupting services worldwide -- an issue traced back to hackers infiltrating networks through IoT devices, including wireless routers and connected cameras. Similarly, in 2020, an IoT data breach occurred when a cybersecurity expert took advantage of a massive Bluetooth vulnerability and hacked a Tesla Model X in less than 90 seconds without so much as triggering an alarm.

Safeguarding IoT devices and the networks they connect to can be challenging due to the variety of devices and vendors, as well as the difficulty of adding security to resource-constrained devices. In the case of the Mirai botnet, the problem was traced back to the use of default passwords on the hacked devices.

Suggested IoT security measures include the following:

- Authentication and authorization and identity management.
- Cryptography.
- Encryption.
- Network segmentation.
- Strong passwords.

Concerned by the dangers posed by the rapidly growing IoT attack surface, the FBI released the public service announcement FBI Alert Number I-091015-PSA in September 2015, which is a document outlining the risks of IoT devices, as well as protections and defense recommendations.

In December 2020, the IoT Cybersecurity Improvement Act of 2020 was signed into law by former President Donald Trump. This law directed the National Institute of Standards and Technology (NIST) to develop and publish standards and guidelines on the use and management of IoT devices. Although these standards were originally intended for use by federal agencies, NIST developed in 2022 a pilot program for IoT security device labeling for consumers. Using NIST's criteria, in 2023, the Biden administration launched

the U.S Cyber Trust Mark, which aims to provide U.S. consumers with labelled products that meet these established security criteria.

Regardless of whether an organization already has IoT devices in use or if they're considering adopting IoT devices, they should ensure they're prepared to handle the unique security challenges presented by IoT devices.

IoT device trends and anticipated growth

The latest IoT Analytics "State of IoT—Spring 2023" report predicts that by 2027, there will be more than 29 billion IoT connections. Although this growth will continue for years to come, the number of devices could fluctuate depending on chipset supply chains and the potential for technological supply shortages.

The key to making effective use of IoT devices is to make sure to start an IoT strategy on the right foot and to understand how the edge and IoT are intertwined with one another.

Benefits of a powerful IoT device solution

The right IoT device solution is a force multiplier. With tools for connecting, integrating and monitoring your devices, your ability to build smart equipment using IoT devices grows exponentially. You can turn real-time data into insights, opportunities and innovations that enable you to evolve new business models and deliver new customer-facing services.

Software AG's Cumulocity IoT platform enables businesses to quickly deploy IoT applications, collect and act on data and integrate IoT with a wide variety of devices and enterprise applications.

The Cumulocity IoT platform allows you to connect and monitor equipment to deliver new services to customers, understand and streamline business operations, or to deliver scalable IoT services to internal and external customers. It is designed to give you complete business visibility and control of all the remote assets in your organization, from the system level down to individual machines and individual sensors. With low-code / no-code tools to build IoT applications and analyze data, it empowers your entire organization to take advantage of IoT insights.

REFERENCES:

1. Gillis, Alexander (2021). "What is internet of things (IoT)?". IOT Agenda. Retrieved 17 August 2021.
2. Brown, Eric (20 September 2016). "21 Open Source Projects for IoT". Linux.com. Retrieved 23 October 2016.

3. "Internet of Things Global Standards Initiative". ITU. Retrieved 26 June 2015.
4. Hendricks, Drew (10 August 2015). "The Trouble with the Internet of Things". London Datastore. Greater London Authority. Retrieved 10 August 2015.
5. "The 'Only' Coke Machine on the Internet". cs.cmu.edu. Carnegie Mellon University. Retrieved 10 November 2014.
6. "Internet of Things Done Wrong Stifles Innovation". InformationWeek. 7 July 2014. Retrieved 10 November 2014.
7. Mattern, Friedemann; Floerkemeier, Christian (2010). "From the Internet of Computer to the Internet of Things" (PDF). Informatik-Spektrum. 33 (2): 107–121. Bibcode:2009InfSp..32..496H. doi:10.1007/s00287-010-0417-7. hdl:20.500.11850/159645. S2CID 29563772. Retrieved 3 February 2014.
8. Weiser, Mark (1991). "The Computer for the 21st Century" (PDF). Scientific American. 265 (3): 94–104. Bibcode:1991SciAm.265c..94W. doi:10.1038/scientificamerican0991-94. Archived from the original (PDF) on 11 March 2015. Retrieved 5 November 2014.
9. "Internet of Things – An action plan for Europe" (PDF). ec.europa.eu. Commission of the European Communities. 18 June 2009. COM(2009) 278 final.
10. Wood, Alex (31 March 2015). "The internet of things is revolutionizing our lives, but standards are a must". The Guardian.
11. Industrial Informatics (INDIN). pp. 1065–1068. doi:10.1109/INDIN.2016.7819322. ISBN 978-1-5090-2870-2. S2CID 5554635.
12. "Everything You Need to Know About IoT & Industrial Internet of Things". Archived from the original on 24 January 2022. Retrieved 5 July 2022.