INTERNET OF THINGS

What is IoT?

- It refers to the interconnection of physical devices, such as appliances and vehicles, that are embedded with software, sensors, and connectivity which enables these objects to connect and exchange data.
- This connectivity enables these objects to connect and exchange data. technology allows for the collection and sharing of data from a vast network of devices, creating opportunities for more efficient and automated systems.

THE HISTORY OF INTERNET OF THINGS (IoT)

Predecessors to IoT

- The term "Internet of Things" was coined by Kevin Ashton in 1999, but the idea had roots in earlier developments.
- In the 1980s and 1990s, researchers began exploring the concept of embedding sensors and connectivity into objects. For example, a Coca-Cola vending machine at Carnegie Mellon University was connected to the internet in 1982 to monitor inventory and temperature.

The Early 2000s

- Kevin Ashton (the guy who came up with the name “Internet of Things”) believed Radio Frequency Identification (RFID) was a prerequisite for the Internet of Things — primarily as an inventory tracking solution.
- In 2002-2003, Walmart and the US Department of Defense were the first large organizations to embrace Ashton’s model of tracking inventory using tagging, RFID, and the Internet of Things.
- The Ring doorbell was developed in 2011 by Jamie Siminoff because he wanted to see who was at his door while he was in the garage, working. He couldn’t hear the doorbell from the garage and kept missing deliveries.

IoT Getting Smarter

- "Smart cities" can use the IoT to reduce waste and maximize the efficient use of energy. The IoT can also be used to streamline traffic flows and locate available parking.
- In 2012, The Swiss Federal Office of Energy started a pilot program called "Smart City Switzerland." They brought representatives from universities, business, and public administration together to discuss new ideas for the urban environment. Smart City Switzerland has over sixty projects underway and supports new scientific partnerships and innovation. (Smart City Switzerland has evolved into something quite impressive.)

The Industrial Internet of Things (IoT)

- The Industrial Internet of Things (IIoT) is an extension of the IoT, and uses actuators and smart sensors, which are networked together with a company's industrial applications. The goal is to give industries greater efficiency and reliability. The IIoT includes robotics and software-defined production processes.

The Internet of Things Becomes a Part of Life

- By the year 2013, the IoT had become a system using multiple technologies, ranging from the Internet to wireless communication and from micro-electromechanical systems (MEMS) to embedded systems.

    Heart Monitor Implant
    Biochip Transponder

The IoT Goes Mobile – 2015

- Smartphones are part of the IoT and have become an important communications tool for many individuals.
- The healthcare industry has also taken advantage of this trend.
- Cars and trucks are already loaded with sensors and technology, including OBD (on-board diagnostics) and GPS.
- Self-driving cars are new members of the IOT.

PROS AND CONS OF INTERNET OF THINGS (IoT)

PROS

1. Easy to Access

- The devices connected to the Internet can be easily accessed from anywhere in the world. All you need is a stable internet connection, and you will be able to control your devices from any corner of the globe.

2. Increased Efficiency

- IoT has made our lives easier and has increased the efficiency of various tasks. For instance, you can now control the temperature of your room from your smartphone while you are on your way back home. This saves you the hassle of manually adjusting the temperature when you reach home.

3. Improved Quality of Life

- IoT has also contributed to improving the quality of life for people with disabilities. There are several smart devices explicitly designed for people with disabilities. Thus, so are the number of pros of Internet of Things in everyday life. These devices make it possible for them to live independent life.

4. Increased Safety and Security

- One of the major benefits of IoT is that it has increased the safety and security of homes and offices. With the help of IoT, people can now monitor their premises from anywhere in the world. This helps you to keep an eye on your belongings even when you are not at home.

5. Greater Convenience

- IoT provides greater convenience as people can now control all the devices in the home or office from a single device. You no longer need to carry a bunch of remote controls everywhere you go.

6. **Improved Communication**

- IoT has also improved communication among different devices. With the help of IoT, various devices can now share data and information. This helps make better decisions as all the relevant information is available in one place.

7. **Reduced Costs**

- IoT has also helped in reducing the costs of various tasks. For instance, with the help of IoT, you can now track your vehicles and save on fuel costs. Similarly, you can also reduce the costs of maintaining your homes by using smart devices that help save energy.

CONS

1. **Security Issues**

- One of the biggest concerns of IoT is security. As more and more devices are connected to the Internet, the chances of data theft and hacking are also increasing.

2. **Privacy Issues**

- That's a sure and dire problem with Internet of things, and that's user privacy. With the help of IoT, companies can now track your movements and collect a lot of data about you. This raises serious concerns about your right to privacy.

3. **Dependence**

- IoT is also creating a dependence on technology. As users become more reliant on smart devices, they are losing their ability to do things independently. This can lead to severe problems if the technology fails or gets hacked.

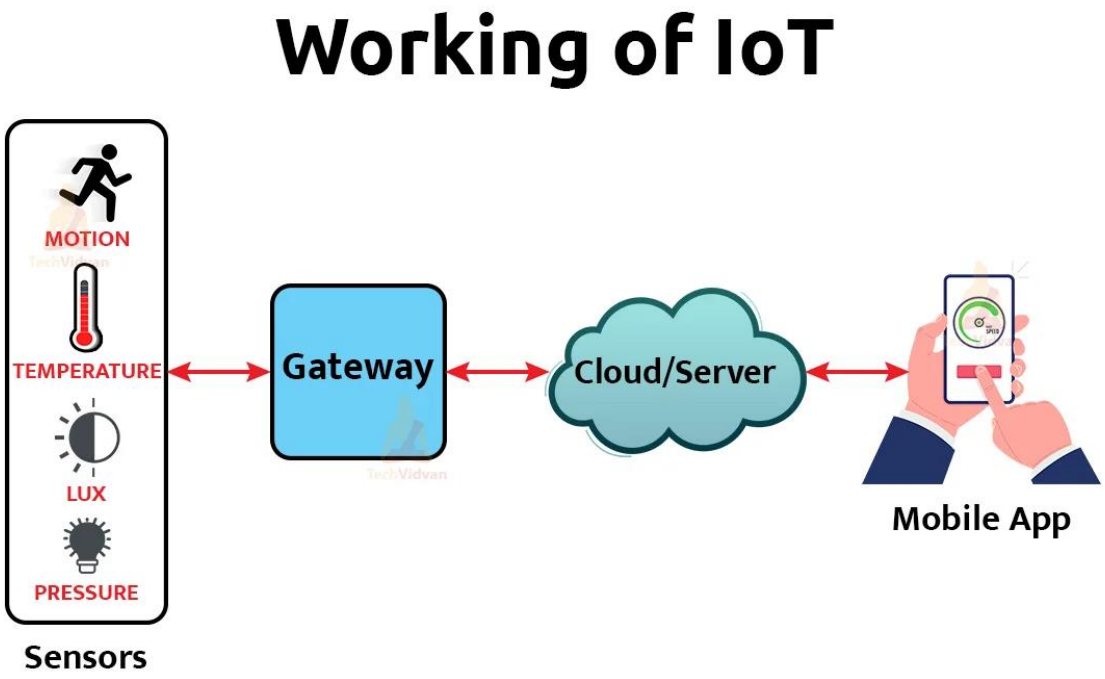
4. **High costs**

- One of the biggest cons of Internet of Things is that it can be quite expensive to implement. The cost of installing and maintaining the infrastructure needed for IoT can be quite high.

5. Complexity

- IoT is also quite complex to understand, especially for those who are not tech-savvy. As the number of devices connected to the internet increases, the system's complexity also increases. This can make it difficult for people to understand and use.

How IOT Works



IoT devices have sensors embedded into them. These sensors are capable of sensing their surroundings. The devices store the information in some form of data. These devices include appliances such as mobile phones, coffee machines, microwaves, geysers, fire alarms, Air conditioners, cars and so on.

The sensors embedded in these devices constantly emit data about the surrounding and on the working information of these devices. IoT serves as a platform to dump all the data collected by these devices.

IoT platform includes cloud servers and large databases. The IoT platform acts on the data. It integrates and processes the information. Further, the platform analyses the data

thoroughly to gather important details. The platform then sends back instructions based on the data provided.

Finally, the data aggregation is shared with other devices for better performance in the future. It is also done for improved user experience.

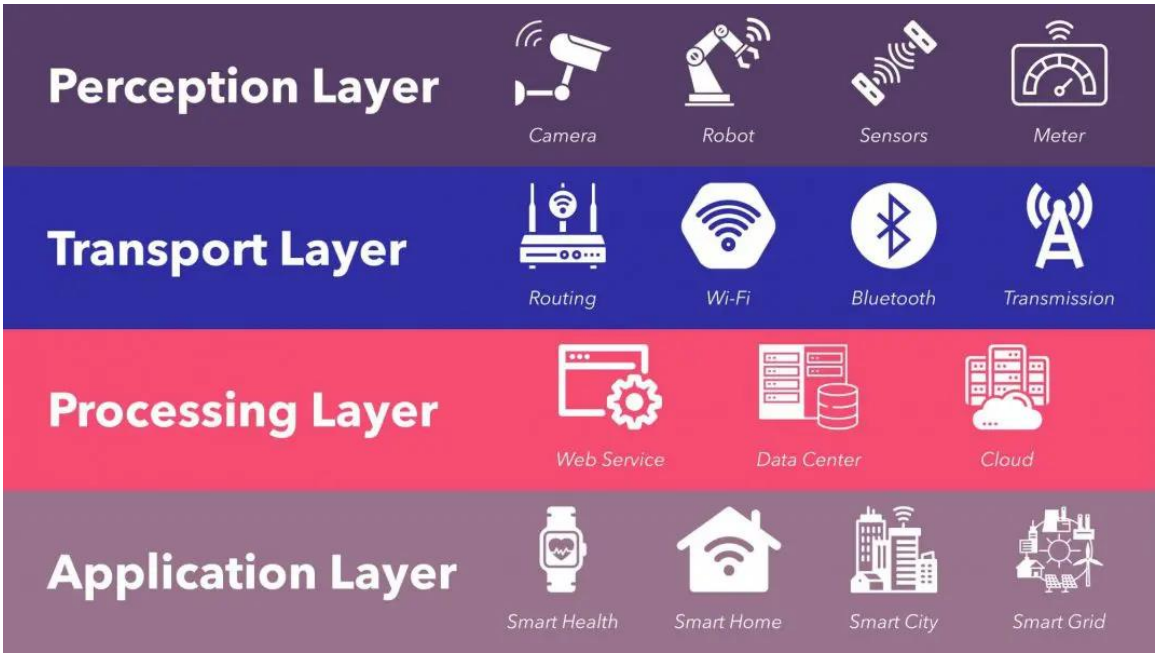
ARCHITECTURE OF INTERNET OF THINGS (IoT)

IoT Architecture

- IoT architecture is the structure enabling internet-connected devices to communicate with other devices.

LAYERS OF INTERNET OF THINGS ARCHITECTURE

Main layers of IoT Architecture



Perception Layer

- The perception layer is the bottommost layer of the IoT architecture and includes the physical devices or sensors that gather data from the surrounding environment. These devices can be various sensors, actuators, RFID tags, cameras, or any other sensing device capable of detecting and measuring different parameters like temperature, humidity, motion, light, etc.

Network Layer

- The network layer facilitates the communication and connectivity between the devices in the IoT ecosystem. It consists of various networking technologies, protocols, and infrastructure components like routers, gateways, switches, and wireless networks (Wi-Fi, Bluetooth, Zigbee, cellular networks, etc.).

Processing Layer

- A fundamental component of an IoT system architecture is its processing layer, also called the middleware layer, which typically leverages many connected computers simultaneously, in the form of cloud computing, to deliver superior compute, storage, networking, and security performance.
- An IoT system typically handles huge volumes of data, generated by numerous edge devices, at multiple sites on the edges of the network. The 'middleware' of the processing layer utilizes a three-stage approach to prepare this data for the application layer:
    1. Data Accumulation: middleware correctly identifies and assigns different data types to the appropriate storage. Unstructured data, such as audio and video streams and images, typically require more storage space and are housed in data lakes. Whereas structured data, comprising instrument readings, log values, and measurements (telemetry data) are more space-efficient and are stored in data warehouses.
    2. Data Abstraction: involves aggregating data from multiple sources, as well as ensuring that data is converted into a format that can be "read" by the software of the application layer.
    3. Data Analysis: employs machine learning (ML) or deep learning algorithms, which are specialized in detecting patterns within large and seemingly random data sets.

Application Layer

- The application layer focuses on processing and analyzing the data collected by the perception layer. It involves data storage, data management, and data processing components, such as cloud platforms, edge computing devices, and data analytics tools.

Business Layer

- Patterns decoded at the application level can be used to further distill business insights, project future trends, and drive operational decisions that improve the

efficiency, safety, cost-effectiveness, customer experience, and other important aspects of business functionality. Indeed, all of this can be accomplished at the business layer of an IoT system architecture.

Security Layer

- Security is one of the most important requirements for an IoT system architecture. Ironically, it also happens to be one of the key challenges facing IoT architecture, and IoT devices themselves. Broadly, the IoT security layer comprises three main aspects:
    1. Equipment Security: involves the actual IoT devices and protecting these endpoints from malware and hijacks.
    2. Cloud Security: with most IoT data being processed in the cloud, cloud security is crucial to prevent data leaks.
    3. Connection Security: focused on securing data transmitted across networks, primarily with encryption. The transport layer security (TLS) protocol is considered the benchmark for IoT connection security.

INTERNET OF THINGS TOOLS AND PLATFORMS

What is IoT tools and platforms?

- IoT tools and platforms refer to software frameworks, development kits, and cloud-based services that facilitate the development, deployment, and management of Internet of Things (IoT) solutions. These tools and platforms provide a set of functionalities and services that help developers and organizations build, connect, monitor, and analyze IoT devices and data.

Internet of Things Tools and Platforms

1. **Software Development Kits (SDKs):** SDKs provide libraries, APIs, and tools that enable developers to program IoT devices, create applications, and interact with IoT platforms. They often include device-specific features and protocols to simplify device integration.
2. **Hardware Development Kits (HDKs):** HDKs are physical kits that include development boards, sensors, actuators, and other components needed to build and prototype IoT devices. They often come with documentation, sample code, and reference designs.

3. **Integrated Development Environments (IDEs):** IDEs are software tools that provide a programming environment for writing, debugging, and testing code. IoT-specific IDEs often offer features tailored for IoT development, such as device simulation, code generation, and device management.
4. **Connectivity Protocols:** IoT tools may include support for various connectivity protocols like Wi-Fi, Bluetooth, Zigbee, Lora WAN, cellular (3G, 4G, or 5G), and MQTT. These protocols allow IoT devices to communicate with each other and connect to cloud platforms.
5. **Cloud Platforms:** Cloud-based IoT platforms provide the infrastructure and services to manage and analyze IoT data. They offer features like device management, data storage, data analytics, real-time monitoring, security, and scalability. Developers can often use APIs and SDKs to integrate their devices and applications with the cloud platform.
6. **Data Analytics and Visualization Tools:** IoT platforms often provide tools for analyzing and visualizing the data generated by IoT devices. These tools help derive insights, detect patterns, and make data-driven decisions. They may include features like dashboards, reporting, machine learning, and predictive analytics.
7. **Device Management Tools:** IoT platforms typically offer device management capabilities that allow users to remotely monitor, configure, and update IoT devices. These tools help ensure the health, security, and performance of the deployed devices.
8. **Security and Authentication:** IoT tools and platforms include security features to protect IoT devices and data from unauthorized access, tampering, and other threats. These features may include authentication, encryption, secure communication protocols, and access control mechanisms.
9. **Integration with Third-Party Services:** Many IoT platforms provide integration with other services, APIs, and frameworks, enabling developers to connect their IoT solutions with external systems, databases, cloud services, or enterprise applications.

APPLICATIONS AREAS OF INTERNET OF THINGS (IoT)

Smart Home

- IoT devices automate and control home functions like lighting, temperature, security, and appliances. Users can monitor and control their homes remotely through apps or voice commands.

Smart Door Access Control => Smart locks and access systems allow secure entry using mobile apps or web interfaces. Users can grant access remotely and lock doors when needed.

Smart Lighting => Energy-saving and customizable lighting controlled via smart hubs or apps. Motion and light sensors activate lights when someone enters or when ambient light is low.

Automated Gate and Garage => Smart sensors enable convenient control of gates and garages using mobile devices.

Smart Thermostats => Internet-connected thermostats controlled via apps or smart hubs for efficient temperature and humidity control.

Traffic Management => Analyzing traffic data helps identify trends, inform commuters, and suggest alternative routes to avoid congestion.

Smart Street Lighting => Energy-efficient lighting that adjusts intensity based on presence, reducing energy waste and aiding emergencies.

Pollution Monitoring => Smart sensors detect air quality changes, collecting data for continuous monitoring and alerting authorities.

Smart Parking Solutions => Real-time availability updates through sensors, enabling efficient parking management.

Water/Waste Management => IoT systems analyze waste production, predict waste levels, and optimize water consumption in growing cities.

Wearable Technology

- Smartwatches and fitness bands improve healthcare monitoring, location tracking, and early disease detection using sensors and apps.

Healthcare

- IoT enhances medical procedures, remote monitoring, data accuracy, and patient satisfaction, reducing errors and improving efficiency.

Autonomous Driving

- IoT-enabled sensors and AI algorithms improve safety and efficiency in self-driving cars and connected vehicles.

Agriculture and Smart Farming

- IoT sensors optimize irrigation, greenhouse environments, and animal tracking, reducing water waste and increasing productivity.

Industrial IoT for Farming

- IoT streamlines supply chain monitoring, automation, product development, quality testing, and cost-effective factory management.

Disaster Management

- IoT sensors detect emergencies like fire, smoke, or high CO2 levels, sending alerts for immediate response and evacuation.

Logistics and Fleet Management

- Smart sensors monitor GPS location, temperature, humidity, and shock during transportation, improving efficiency and customer communication.

Smart Grids and Energy Management

- IoT and smart meters provide data for optimizing energy distribution, reducing carbon emissions, and enabling cost-saving measures.

Big Data Analytics

- IoT generates vast amounts of data for analysis, enabling AI and machine learning algorithms to make informed decisions and improve various applications.

REFERENCES

Foote, K. D. (2023, March 28). A Brief History of the Internet of Things - DATAVERSITY. DATAVERSITY.

https://www.dataversity.net/brief-history-internet-things/

GeeksforGeeks. (2023). Architecture of Internet of Things IoT. *GeeksforGeeks*.

https://www.geeksforgeeks.org/architecture-of-internet-of-things-iot/

Gil Press. (2014, June 18). A Very Short History Of The Internet Of Things. Forbes.

https://www.forbes.com/sites/gilpress/2014/06/18/a-very-short-history-of-the-internet-of-things/?sh=7e8bd20110de

Rajiv. (2023). Applications of Internet of Things (IoT). RF Page.

https://www.rfpage.com/applications-of-internet-of-things-iot/

Simmons, A. (2023, January 24). Internet of Things (IoT) Architecture: Layers Explained. *Dgtl Infra*.

https://dgtlinfra.com/internet-of-things-iot-architecture/#:~:text=IoT%20architecture%20is%20the%20structure,(e.g.%2C%20software

TheTechPrint. (2022). Pros and Cons of Internet of Things. The Tech Print.

https://thetechprint.com/pros-and-cons-of-internet-of-things

Team, T. (2023). How IOT works?. TechVidvan.

https://techvidvan.com/tutorials/how-iot-works/

INTERNET OF THINGS (IoT)

Leader: DE RUEDA, Allen

Members:

ALBAY, NJ Brix

BONDOC, Elyda Sofia

PADILLA, Adrianne Kim