[12pt]report geometry graphicx xcolor titlesec float

Chapter 1

Generality

1.1 Internet of Things Technology (IoT)

1.1.1 Definition

IoT, or Internet of Things, is a system of interconnected physical devices, vehicles, buildings, and other objects that have been embedded with sensors, software, and network connectivity to collect and exchange data. IoT technology provides real-time data for monitoring and controlling processes and functions, with potential to revolutionize industries like manufacturing, healthcare, transportation, and energy. The implementation of IoT poses challenges such as heterogeneity, complexity, poor interoperability, resource constraints, and privacy concerns, which must be addressed to fully realize the benefits of this technology.[**?**]

1.1.2 Architectures

The Internet of Things (IoT) is a technology that includes three main layers the Perception Layer, Transmission Layer and Application Layer.[**?**]

1.1.2.1 Perception Layer

The Perception Layer is the lowest layer in the IoT architecture, sometimes called the Device, Sensory, or Recognition Layer. It is responsible for sensing, identifying, and communicating with the physical world in a digital format. This layer captures data with little human intervention. The Perception

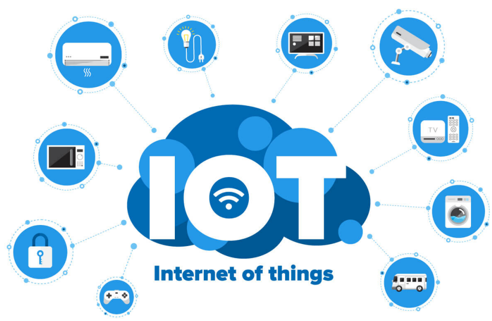

Figure 1.1: A sample image of IoT devices[?].

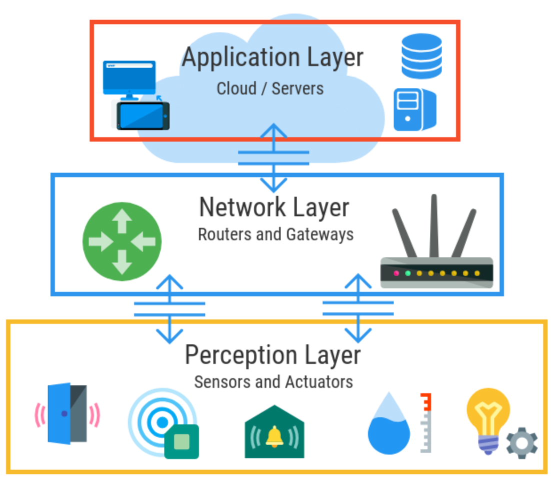

Figure 1.2: The fundamental Three Layer IoT Architecture [?].

Layer of the IoT architecture consists of the Perception Nodes and the Perception Network.

Perception Nodes

The Perception Nodes refer to the physical devices such as sensors, actuators, and controllers that form a network to collect data and control objects. This network can be established through various technologies, including RFID readers, QR code or Barcode readers, GPS devices, Bluetooth devices, and various sensors. The Perception Nodes identify objects, collect data from the environment, and control objects.

Perception Networks

The Perception Network communicates with the Transmission Network, securely transmitting data collected by the Perception Nodes to gateways for further transmission and sending control signals to controller devices through wired or wireless communication mediums.

1.1.2.2 Transmission (Network) Layer

The Transmission Layer is an important part of the IoT architecture that sits between the Perception and Application Layers. It's responsible for integrating various networks, technologies, and protocols to transmit data from Perception Nodes to higher level decision-making units. The data is transferred through wired or wireless communication channels, and the layer provides functionalities for network management. The Transmission Layer is also responsible for providing necessary support for analyzing, encoding, aggregating and data mining. It can be divided into three sub-layers below :

- Access Network
- Core Network
- Local and Wide Area Network

1.1.2.3 Application Layer

The Application Layer is the highest layer of the IoT architecture, visible to the end user. Its purpose is to manage and provide applications globally based on the information collected by the Perception Layer, which is processed by the Information Processing Unit. This layer provides access to personalized services for end-users over the network through the use of various handheld devices and terminal equipment. It can be divided into two sub-layers: Application Support Layer and IoT Applications.
The Application Support Layer is located just above the Transmission Layer, responsible for performing intelligent computations and processing over data. It performs data recognition and filtration to categorize it as valid or invalid, and utilizes middleware, Cloud Computing, and Service Support Platform to provide support services for the applications

1.1.3 Protocoles

IoT protocols are a set of rules that allow electronic devices to exchange and transmit data with each other and the internet. These protocols can be classified into two categories: IoT network protocols and IoT data protocols. Network protocols help connect IoT devices with other edge devices or the internet, while data protocols focus on exchanging information, each category has its own set of protocols that come with unique features, which we will examine in the following section.[**?**]

1.1.3.1 IoT Network Protocols

Wi-Fi

Wi-Fi, defined by the IEEE 802.11 standard, is a widely used wireless LAN protocol for transmitting large volumes of data over reasonable distances. Low-power IoT devices avoid it due to high power consumption.

Bluetooth

Bluetooth is a short-range wireless technology standard for exchanging data between devices over short distances. It's used in IoT to connect small, battery-powered sensors to gateways or other smart devices. With limited transmission power of 2.5 milliwatts, it has a short range of up to 10 metres.

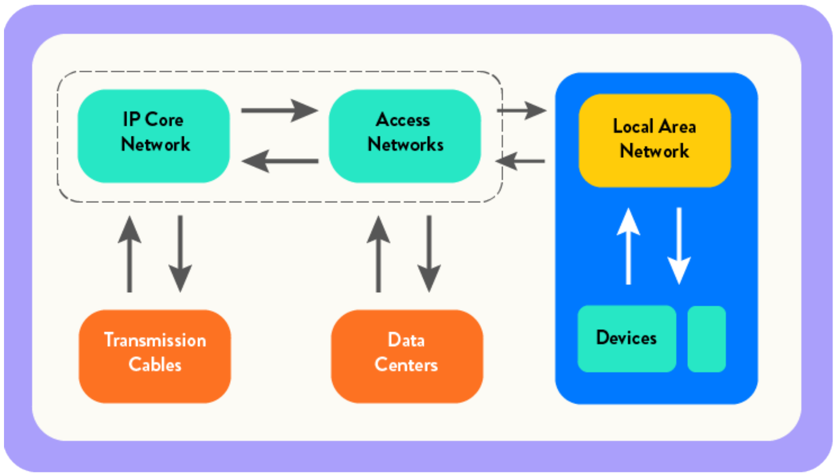

Figure 1.3: illustration showing a network system diagram [?].

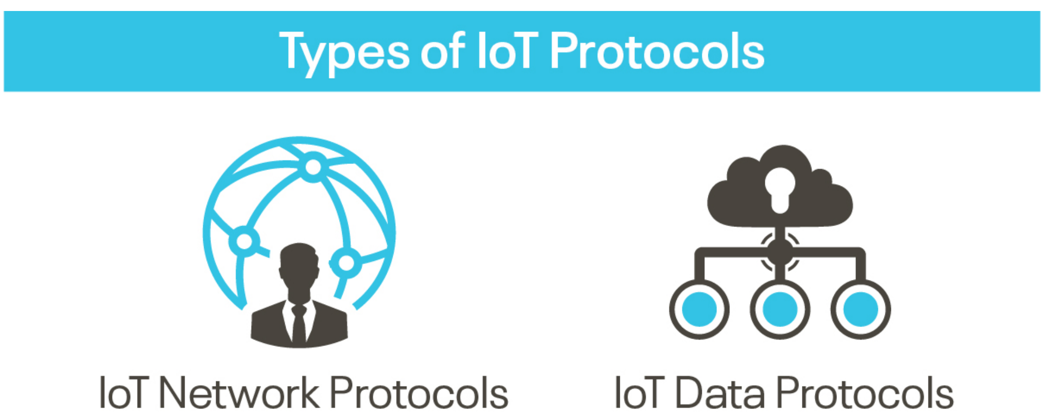

Figure 1.4: IoT Protocols [?].

ZigBee

ZigBee is a wireless network technology used in home or building automation settings. It's low-cost, low-power and reliable, and supports multiple network topologies. ZigBee devices combine application, logical, and physical types. The standard was ratified in the early 2000s.[**?**]

LoRaWAN

The LoRaWAN is a Low Power, Wide Area (LPWA) protocol designed to attach battery-powered gadgets to the net in regional, countrywide or international networks. It addresses key IoT requirements like secure two-way communication, mobility, and localization services.[**?**]

1.1.3.2 IoT Data Protocols

MQTT

The Message Queue Telemetry Transport (MQTT) protocol is a lightweight, open, and simple client-server messaging transport designed for easy implementation. It uses a publish/subscribe message pattern that allows for one-to-many message distribution and is agnostic to the content of the payload[**?**]. The protocol offers three levels of message delivery quality of service, allowing for greater control over network traffic. MQTT is an excellent fit for IoT communication, requiring minimal memory and processing power. Additionally, the protocol is designed for reliability and scalability, with Transport Layer Security enabling security and adaptive connectivity.[**?**]

CoAP

Constrained Application Protocol (CoAP) is a specialized web transfer protocol designed for Machine-to-Machine (M2M) applications, such as smart city and building automation, with constrained nodes and networks. CoAP enables resource-constrained devices to communicate with the wider Internet using lightweight packets, thereby reducing network congestion, saving battery power and storage space, and improving the IoT lifecycle.[**?**] CoAP's request and response interaction model between application end points, built-in discovery services, and support for key Web concepts such as URIs and Internet media types make it an ideal protocol for low-power, low-bandwidth

Figure 1.5: The IoT Network Protocols [?].

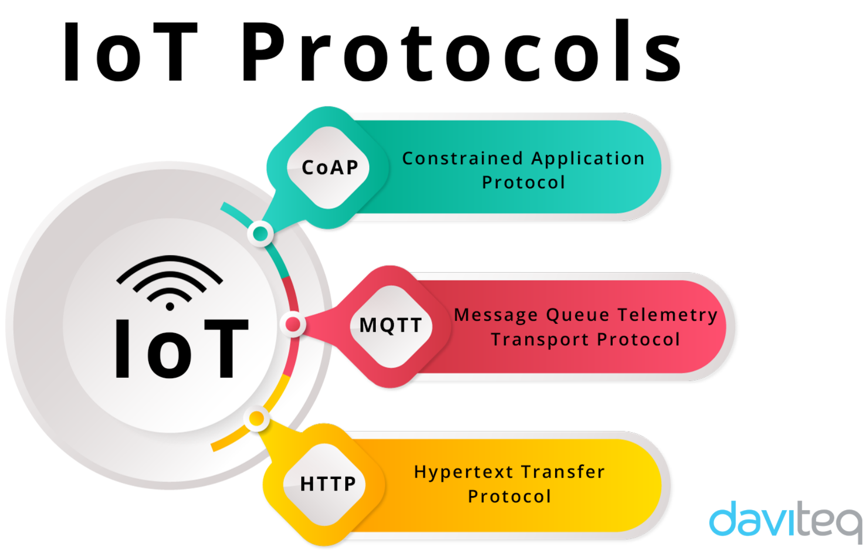

Figure 1.6: Some data protocols for IoT [?].

network connectivity. CoAP is designed to integrate seamlessly with HTTP while meeting specialized requirements such as multicast support and simplicity for constrained environments, with a high packet error rate and typical throughput of 10 kbps[?].

AMQP

Advanced Message Queuing Protocol (AMQP) is a protocol designed for corporate messaging, offering a range of features related to messaging such as reliable queuing, flexible routing, and transactions.[?]AMQP is a binary protocol that requires a fixed 8-byte header and has a maximum message payload size determined by the broker or programming technology being used. The maximum size of the message payloads is generally small.[?]Its use of TCP and TLS/SSL for security makes it a secure and trustworthy protocol for IoT applications[?].Overall, AMQP plays a vital role in enabling communication and coordination among diverse devices in the IoT domain.

HTTP

Hyper Text Transport Protocol (HTTP) is widely used as a web messaging protocol for Internet of Things (IoT) applications. Developed jointly by the IETF and W3C, it supports the request/response RESTful web architecture and uses Universal Resource Identifiers (URI) for data exchange[?]. Servers send data through URIs, and clients receive data through specific URIs. HTTP is a text-based protocol that does not define the size of header and message payloads, which depends on the web server or programming technology. It uses TCP as the default transport protocol and TLS/SSL for security.Despite now no longer defining QoS, it gives numerous functions together with continual connections, request pipelining,and chunked transfer encoding that make it an ideal protocol for various IoT applications.

1.1.4 Applications

The Internet of Things (IoT) allows us to access clever services in many areas of life. However, because the devices are so varied and interconnected, there can be challenges to overcome. These services include things like transportation, environmental monitoring, healthcare, weather and more.

Smart homes

IoT devices such as smart thermostats, lighting systems, and security cameras can be controlled remotely using a smartphone or voice command, making our homes more comfortable, secure, and energy-efficient.

Healthcare

IoT devices such as wearables and remote patient monitoring systems can track and transmit health data, allowing doctors and caregivers to monitor patients' health in real-time and provide timely interventions.

Transportation

IoT-enabled vehicles can communicate with each other and with infrastructure, enabling safer and more efficient transportation, and helping to reduce traffic congestion.

Agriculture

IoT sensors may be used to reveal soil moisture, temperature, and different environmentalfactors, allowing farmers to optimize crop yields and reduce water and fertilizer usage.

Manufacturing

IoT-enabled sensors and analytics tools can be used to monitor machine performance and detect maintenance issues, reducing downtime and improving production efficiency.

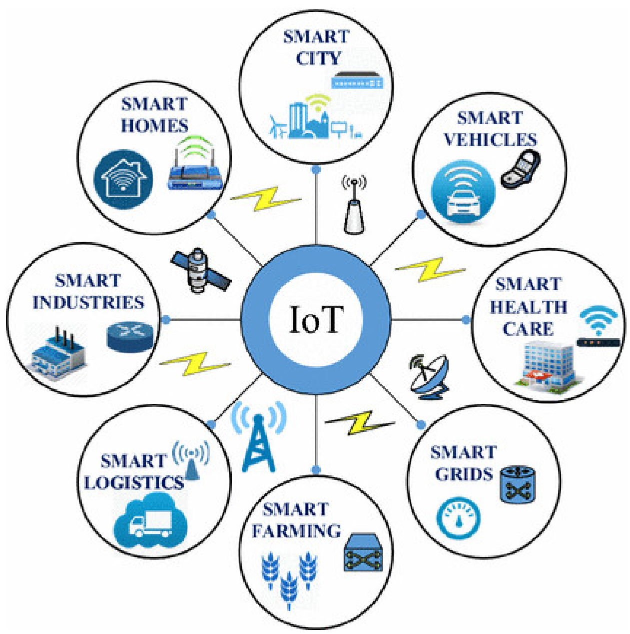

Figure 1.7: IoT Applications domains [?].

Contents

List of Figures

List of Tables

Bibliography

[1] Yvan Duroc and Smail Tedjini. Rfid: A key technology for humanity. *Comptes Rendus Physique*, 19(1-2):64–71, 2018.

[2] SCHMIDT. Rfid solutions. `http://www.schmidt.com.cn/uploadfiles/2018/06/20180614160652652.png`, 2020.

[3] Chang-He Li, Keng-Weng Lao, and Kam-Weng Tam. A flooding warning system based on rfid tag array for energy facility. In *2018 IEEE International Conference on RFID Technology & Application (RFID-TA)*, pages 1–4. IEEE, 2018.

[4] Hugo Landaluce, Laura Arjona, Asier Perallos, Francisco Falcone, Ignacio Angulo, and Florian Muralter. A review of iot sensing applications and challenges using rfid and wireless sensor networks. *Sensors*, 20(9):2495, 2020.

[5] easyRFID. Rfid technology: what it is, how it works and what it is for, 2022.

[6] Yvan Duroc. From identification to sensing: Rfid is one of the key technologies in the iot field. *Sensors*, 22(19):7523, 2022.

[7] Vipul Chawla and Dong Sam Ha. An overview of passive rfid. *IEEE Communications Magazine*, 45(9):11–17, 2007.

[8] AUCXIS rfidsolutions. Rfid – identify, read and process unique information, 2023.

[9] easyrfid. `https://www.easyrfid.it/en/tecnologia-rfid/`, 2022. Accessed on February 15, 2023.

[10] rfid4u. Explore rfid basics and resources rfid basics - the rf in rfid, 2023.

[11] ColetteM Girard. *Processing of remote sensing data*. Routledge, 2018.

[12] Antoine Denis. Travaux pratiques de télédétection spatiale i. 2020.

[13] Paul Mather and Brandt Tso. *Classification methods for remotely sensed data*. CRC press, 2016.

[14] Charles Elachi. Spaceborne radar remote sensing: applications and techniques. *New York*, 1988.

[15] Yuting Zhou, K Colton Flynn, Prasanna H Gowda, Pradeep Wagle, Shengfang Ma, Vijaya G Kakani, and Jean L Steiner. The potential of active and passive remote sensing to detect frequent harvesting of alfalfa. *International Journal of Applied Earth Observation and Geoinformation*, 104:102539, 2021.

[16] Johannes Heisig, Edward Olson, and Edzer Pebesma. Predicting wildfire fuels and hazard in a central european temperate forest using active and passive remote sensing. *Fire*, 5(1):29, 2022.

[17] Xiaoye Tong, Feng Tian, Martin Brandt, Yi Liu, Wenmin Zhang, and Rasmus Fensholt. Trends of land surface phenology derived from passive microwave and optical remote sensing systems and associated drivers across the dry tropics 1992–2012. *Remote Sensing of Environment*, 232:111307, 2019.

[18] Sarah B Schroeder, Colleen Dupont, Leanna Boyer, Francis Juanes, and Maycira Costa. Passive remote sensing technology for mapping bull kelp (nereocystis luetkeana): a review of techniques and regional case study. *Global Ecology and Conservation*, 19:e00683, 2019.

[19] SKYRORA. What is satellite remote sensing?, 2021.

[20] Silvia Liberata Ullo and Ganesh Ram Sinha. Advances in iot and smart sensors for remote sensing and agriculture applications. *Remote Sensing*, 13(13):2585, 2021.

[21] Karsten Schulz, Ronny Hänsch, and Uwe Sörgel. Machine learning methods for remote sensing applications: an overview. *Earth resources and environmental remote sensing/GIS applications IX*, 10790:1079002, 2018.

[22] Khai Loong Chong, Kasturi Devi Kanniah, Christine Pohl, and Kian Pang Tan. A review of remote sensing applications for oil palm studies. *Geo-spatial Information Science*, 20(2):184–200, 2017.

[23] Ranganath R Navalgund, V Jayaraman, and PS Roy. Remote sensing applications: An overview. *current science*, pages 1747–1766, 2007.

[24] L Karthikeyan, Ila Chawla, and Ashok K Mishra. A review of remote sensing applications in agriculture for food security: Crop growth and yield, irrigation, and crop losses. *Journal of Hydrology*, 586:124905, 2020.

[25] Stuart J Russell. *Artificial intelligence a modern approach.* Pearson Education, Inc., 2010.

[26] D Manning Christopher and Schütze Hinrich. Foundations of statistical natural language processing. 1999.

[27] Christopher M Bishop and Nasser M Nasrabadi. *Pattern recognition and machine learning.* Springer, 2006.

[28] Galit Shmueli. To explain or to predict? 25(3):289–310, 2010.

[29] Ethem Alpaydin. Introduction to machine learning, 2'nd ed, 2010.

[30] Kevin P Murphy. *Machine learning: a probabilistic perspective.* MIT press, 2012.

[31] Trevor Hastie, Robert Tibshirani, Jerome H Friedman, and Jerome H Friedman. *The elements of statistical learning: data mining, inference, and prediction*, volume 2. Springer, 2009.

[32] Saleema Amershi, Maya Cakmak, William Bradley Knox, and Todd Kulesza. Power to the people: The role of humans in interactive machine learning. *Ai Magazine*, 35(4):105–120, 2014.

[33] Michael I Jordan and Tom M Mitchell. Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245):255–260, 2015.

[34] Yann LeCun, Yoshua Bengio, Geoffrey Hinton, et al. Deep learning. nature, 521 (7553), 436-444. *Google Scholar Google Scholar Cross Ref Cross Ref*, page 25, 2015.

[35] Ian Goodfellow, Yoshua Bengio, and Aaron Courville. *Deep learning*. MIT press, 2016.

[36] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. Imagenet classification with deep convolutional neural networks. *Communications of the ACM*, 60(6):84–90, 2017.

[37] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N Gomez, Łukasz Kaiser, and Illia Polosukhin. Attention is all you need. *Advances in neural information processing systems*, 30, 2017.

[38] Alex Graves and Jürgen Schmidhuber. Framewise phoneme classification with bidirectional lstm and other neural network architectures. *Neural networks*, 18(5-6):602–610, 2005.

[39] Volodymyr Mnih, Koray Kavukcuoglu, David Silver, Andrei A Rusu, Joel Veness, Marc G Bellemare, Alex Graves, Martin Riedmiller, Andreas K Fidjeland, Georg Ostrovski, et al. Human-level control through deep reinforcement learning. *nature*, 518(7540):529–533, 2015.

[40] Richard S Sutton and Andrew G Barto. *Reinforcement learning: An introduction*. MIT press, 2018.

[41] Burr Settles. Active learning literature survey. 2009.

[42] Sinno Jialin Pan and Qiang Yang. A survey on transfer learning. *IEEE Transactions on knowledge and data engineering*, 22(10):1345–1359, 2010.