IoT Devices: Classification, Features, and Trends in Modern IoT Systems

Md Hafizur Rahman[1,*], M. Naderuzzaman[2], and Md Masud Reza[3]

[1]HafizLab, Dhaka, Bangladesh
[2]Department of Computer Science and Engineering, Sonargaon University, Dhaka, Bangladesh
[3]Department of Computer Science and Engineering, The People's University of Bangladesh

***Abstract*—The Internet of Things (IoT) has revolutionized the way physical objects interact with digital systems, creating a seamlessly connected environment across various domains. This paper presents a comprehensive overview of modern IoT devices, focusing on their classification, core features, and emerging trends. It examines the technical architecture, connectivity protocols, sensing and communication capabilities, and application-specific design considerations of IoT devices. Furthermore, the study highlights their roles in smart homes, healthcare, agriculture, industrial automation, and environmental monitoring. The paper also addresses critical challenges such as interoperability, security, scalability, and energy efficiency. Finally, future research directions and technological advancements are discussed to provide a holistic understanding of the evolving landscape of IoT systems.**

***Index Terms*—IoT Devices, Sensors, Actuators, Connectivity, Smart Systems, Industry 4.0, Edge Computing, Smart Home**

Received: 8 August 2025, Revised: 25 August 2025
Accepted: 15 September 2025, Published: 30 September 2025
Email of corresponding author: hafizurfpbd@gmail.com

I. Introduction

The Internet of Things (IoT) represents a network of interconnected physical devices that collect, exchange, and process data [1], [2]. These devices, ranging from simple sensors to complex industrial machines, are embedded with electronics, software, and network connectivity, enabling them to interact with the environment[3] and other devices [4].

IoT has emerged as a transformative technology impacting various sectors, including smart homes, healthcare, agriculture, and industrial automation [5]. The ability of devices to sense, communicate, and act in real time has revolutionized how data is collected, analyzed, and utilized [6].

IoT devices play a crucial role in creating smart systems that enhance efficiency, safety, and convenience. In smart homes, IoT enables automation of lighting, temperature, and security systems [6]. In healthcare, IoT devices allow remote patient monitoring and personalized treatment [1]. In agriculture, smart sensors optimize irrigation, soil monitoring, and crop management [5]. Industrial IoT (IIoT) improves production processes, predictive maintenance, and supply chain management [4].

Modern IoT devices are characterized by their connectivity, interoperability, data processing capabilities, and energy efficiency. They can communicate using short-range protocols such as Bluetooth and Zigbee, or long-range technologies like LoRaWAN and NB-IoT [7]. Interoperability and standardized protocols allow heterogeneous devices to work seamlessly within a network, while edge and cloud computing enable efficient data processing and analytics [4].

Despite their benefits, IoT devices also face challenges related to security, data privacy, scalability, and power management [1], [5]. Addressing these challenges is essential to ensure the reliability and sustainability of IoT ecosystems. At the same time, advancements in AI, 5G, and energy-efficient designs present new opportunities for more intelligent and autonomous IoT systems [7].

This paper provides a comprehensive overview of modern IoT devices, focusing on their classification, key features, and emerging trends. By exploring the technical aspects, applications, and challenges of IoT devices, this study aims to provide a foundation for researchers [8], engineers, and practitioners to develop innovative and scalable IoT solutions.

II. Classification of IoT Devices

IoT devices can be classified based on several criteria including their functionality, connectivity, application domain, and power source. Understanding these classifications helps in designing, deploying, and managing IoT systems efficiently.

A. Based on Functionality

IoT devices can be categorized based on their primary functions within an IoT ecosystem. The functionality-based classification helps in understanding how different devices contribute to data acquisition, processing, actuation, and communication within interconnected systems. The major functional categories include sensing devices, actuating devices, processing devices, and communication devices.

a) Sensing Devices: Sensing devices are the most fundamental components of IoT systems, responsible for acquiring data from the physical environment. These devices are equipped with sensors that measure various parameters such as temperature, humidity, pressure, light intensity, motion, and gas concentration. The collected data are typically transmitted to a central node or processing unit for further analysis[9]. Examples of sensing devices include temperature sensors, motion detectors, and air quality monitoring sensors.

b) Actuating Devices.: Actuating devices perform specific physical actions based on control commands or processed sensor data. They serve as the interface between the digital and physical worlds[10], enabling IoT systems to influence their environment. Common actuators include electric motors, solenoid valves, and smart relays, which are used in applications such as automated door locks, irrigation systems, and robotic control. Actuators are crucial in achieving automation and feedback-based control in IoT architectures.

c) Processing Devices.: Processing devices are responsible for computation, decision-making, and local data processing. These devices typically include microcontrollers, embedded processors, or single-board computers capable of executing lightweight algorithms and handling sensor data. Edge computing is often implemented at this layer to minimize latency and reduce network congestion by performing data processing close to the data source. Examples include Arduino, Raspberry Pi, and ESP32-based systems.

d) Communication Devices.: Communication devices are designed to facilitate data exchange between IoT nodes, gateways, and cloud servers. They integrate various communication modules that operate using short-range or long-range wireless technologies such as Wi-Fi, Bluetooth, Zigbee, LoRa, and cellular networks. These devices play a crucial role in enabling seamless connectivity and interoperability among heterogeneous IoT components. Effective communication devices ensure reliable data transmission and synchronization across distributed IoT systems.

B. Based on Communication Range

IoT devices can also be classified according to the communication range they support, which directly influences their energy consumption, data rate, and suitable deployment scenarios. The communication range determines how far devices can transmit data, thereby defining their application in personal, local, or wide-area networks. Broadly, IoT communication technologies can be divided into short-range, medium-range, and long-range categories.

a) Short-Range Devices.: Short-range IoT devices are designed for limited-area connectivity, typically within homes, buildings, or industrial plants. They are characterized by low power consumption, high data rates, and reliable peer-to-peer or mesh communication. Common technologies supporting short-range communication include Bluetooth, Zigbee, Wi-Fi, and Near Field Communication (NFC). These devices are widely used in smart home systems, wearable technology, and industrial automation where proximity-based communication is sufficient[3].

b) Medium-Range Devices.: Medium-range IoT devices operate over extended distances compared to short-range systems and are suitable for applications such as smart campuses, agriculture, and logistics. They balance range and energy efficiency while maintaining moderate data throughput. Typical technologies in this category include Z-Wave, WirelessHART, and LoRa (Long Range). Such devices are often deployed in scenarios where coverage needs to span multiple buildings or several kilometers without relying on cellular infrastructure.

c) Long-Range Devices.: Long-range IoT devices are designed for wide-area communication, enabling connectivity over several kilometers to tens of kilometers. They are commonly used in large-scale deployments such as smart cities, remote monitoring, and industrial IoT applications. Technologies supporting long-range communication include NB-IoT (Narrowband IoT), LTE-M (Long-Term Evolution for Machines), 5G, and satellite-based IoT systems. Although these devices typically consume more power and offer lower data rates, they provide reliable connectivity in geographically dispersed or infrastructure-limited environments.

C. Based on Power Source

The classification of IoT devices based on their power source is essential for understanding their energy requirements, deployment feasibility, and operational longevity. Since IoT devices are often deployed in remote or resource-constrained environments, the choice of power source significantly affects their design, maintenance, and performance. Generally, IoT devices can be categorized as battery-powered, energy-harvesting, or mains-powered systems.

a) Battery-Powered Devices: Battery-powered IoT devices rely on rechargeable or non-rechargeable batteries as their primary source of energy. These devices are suitable for portable and remote applications where access to wired power is limited. The design of such devices emphasizes low power consumption and energy-efficient communication protocols to extend battery life. Typical examples include wearable health monitors, wireless environmental sensors, and asset tracking devices. Although convenient, frequent battery replacement or recharging can be a limitation for large-scale deployments.

b) Energy-Harvesting Devices: Energy-harvesting IoT devices obtain power from ambient environmental sources such as solar radiation, vibration, thermal gradients, or radio frequency (RF) signals. This approach enhances sustainability and enables maintenance-free operation in remote or inaccessible locations. Energy-harvesting devices are increasingly being adopted in environmental monitoring, agriculture, and smart city infrastructures. For example, solar-powered air quality monitors or vibration-powered machinery sensors can operate autonomously for extended periods without manual intervention.

c) Mains-Powered Devices: Mains-powered IoT devices draw electrical energy directly from the grid and are typically used in fixed installations where continuous power is available. These devices support higher computational workloads, constant data transmission, and complex operations that would otherwise be constrained by battery limitations. Common applications include smart home appliances, industrial automation controllers, and surveillance systems. While mains power ensures reliability and high performance, it limits the portability and flexibility of deployment compared to battery- or energy-harvesting-based systems.

D. Based on Deployment Environment

IoT devices can also be categorized according to their deployment environments, which determine their design specifications, communication requirements, and operational constraints. The deployment environment influences the device's durability, connectivity type, and compliance with industry-specific standards. Based on this perspective, IoT devices are generally classified into consumer, industrial, commercial, and infrastructure categories.

a) Consumer IoT Devices.: Consumer IoT devices are primarily designed for personal and household use, focusing on convenience, automation, and user experience. These devices typically feature user-friendly interfaces, wireless connectivity, and integration with mobile applications or cloud platforms. Common examples include smart home appliances, wearable fitness trackers, voice-controlled assistants, and connected entertainment systems. Such devices emphasize affordability and ease of installation but may face challenges related to data privacy and interoperability.

b) Industrial IoT (IIoT) Devices.: Industrial IoT devices are specifically engineered for manufacturing, production, and process automation environments. They are built to operate under harsh conditions involving high temperatures, vibration, or electromagnetic interference. IIoT devices play a vital role in predictive maintenance, real-time monitoring, and process optimization. Examples include programmable logic controllers (PLCs), industrial-grade sensors, and robotic control units. Reliability, scalability, and security are critical attributes for this class of IoT devices.

c) Commercial IoT Devices: Commercial IoT devices are deployed in sectors such as healthcare, retail, logistics, and office environments. These devices support business operations by enabling automation, data analytics, and customer engagement. Typical examples include smart lighting systems, medical monitoring devices, inventory management sensors, and building automation controllers. Commercial IoT systems often require compliance with industry regulations, secure data handling, and integration with enterprise information systems.

d) Infrastructure IoT Devices: Infrastructure IoT devices are used in large-scale systems that support public services, utilities, and urban infrastructure. They are essential components in smart cities, energy grids, and transportation networks. Examples include smart meters, traffic monitoring systems, waste management sensors, and environmental monitoring units. These devices are designed for long-term reliability, remote management, and large-area coverage. The data collected from infrastructure IoT systems play a critical role in improving efficiency, sustainability, and urban planning.

E. Based on Data Processing Location

IoT devices can also be classified according to the location where data processing occurs within the system architecture. The data processing model determines how information is collected, analyzed, and acted upon across different network layers. Depending on computational capabilities, latency requirements, and network constraints, IoT devices are typically categorized as edge devices, fog devices, or cloud-based devices.

a) Edge Devices: Edge devices perform data processing locally, close to the data source, in order to minimize latency and reduce bandwidth usage. These devices are equipped with onboard processors and memory to handle data analytics, filtering, and decision-making before transmitting only relevant information to higher layers. Edge computing enhances real-time responsiveness and is particularly valuable in time-sensitive applications such as autonomous vehicles, industrial automation, and healthcare monitoring. Examples of edge devices include microcontrollers, smart sensors, and embedded gateways[14], [16].

b) Fog Devices: Fog devices serve as an intermediate layer between edge devices and the cloud, providing localized data aggregation, temporary storage, and partial analytics. The concept of fog computing extends the cloud's computational capabilities closer to the network edge, thereby improving scalability and reducing network congestion. Fog devices are commonly used in smart grids, transportation systems, and large-scale sensor networks where distributed processing improves performance and reliability. Typical fog nodes include industrial gateways, routers, or local servers[14].

c) Cloud-Based Devices: Cloud-based IoT devices depend on remote cloud servers for data processing, storage, and management. These devices typically collect raw data and transmit it over the internet to centralized platforms for advanced analytics, visualization, and decision-making. Cloud computing offers virtually unlimited processing power and scalability, enabling complex machine learning and big data operations. Examples include smart home ecosystems and environmental monitoring networks that rely on platforms such as AWS IoT, Microsoft Azure IoT Hub, or Google Cloud IoT Core. However, challenges such as high latency, data privacy, and dependence on continuous connectivity must be carefully addressed in cloud-centric IoT architectures[14].

F. Based on Application Domain

IoT devices can further be categorized based on their application domains, which define the specific areas where they are deployed and the nature of tasks they perform. This classification reflects the diversity of IoT applications across various sectors, ranging from household automation to industrial operations and environmental management. Each domain has distinct requirements in terms of device design, communication protocols, data security, and reliability.

a) Smart Home Devices: Smart home IoT devices are designed to enhance comfort, convenience, and energy efficiency within residential environments. These devices enable automation and remote control of various household systems such as lighting, heating, and security. Common examples include smart thermostats, connected lighting systems, smart locks, and surveillance cameras. Such devices often integrate with cloud-based platforms and voice assistants, allowing users to manage home environments through mobile or web applications.

b) Healthcare Devices: In the healthcare domain, IoT devices play a critical role in remote patient monitoring, diagnostics, and personalized treatment. These devices continuously collect physiological data such as heart rate, blood pressure, and glucose levels, transmitting them to healthcare providers for real-time analysis and decision-making. Examples include wearable fitness trackers, smart glucose monitors, and wireless electrocardiogram (ECG) sensors. IoT-enabled healthcare systems contribute to early disease detection, improved patient outcomes, and reduced hospital readmissions, although they must comply with stringent data security and privacy standards.

c) Agricultural Devices: Agricultural IoT devices are utilized to optimize farming practices through data-driven decision-making. These devices monitor soil moisture, nutrient levels, temperature, and weather conditions to improve crop yield and resource utilization. Examples include automated irrigation controllers, soil health sensors, and livestock tracking systems. The use of IoT in agriculture supports precision farming, reduces water consumption, and enhances sustainability, particularly in resource-constrained regions.

d) Industrial Devices: Industrial IoT (IIoT) devices are employed in manufacturing, logistics, and production systems to enable automation, predictive maintenance, and process optimization. These devices collect real-time data from machines, production lines, and supply chains to improve operational efficiency and reduce downtime. Common examples include vibration sensors, robotic control units, and condition monitoring devices. Industrial IoT systems often integrate with supervisory control and data acquisition (SCADA) systems and employ robust communication protocols to ensure reliability and security in critical environments[15], [17].

e) Environmental Devices: Environmental IoT devices are designed to monitor and manage ecological and atmospheric parameters for sustainable resource management. These devices collect data related to air quality, water quality, noise pollution, and weather patterns. Examples include particulate matter (PM) sensors, gas analyzers, and meteorological monitoring stations. The collected data are used in applications such as urban pollution management, disaster prediction, and climate research. Environmental IoT devices are vital for supporting smart city initiatives and addressing global environmental challenges.

III. Key Features of IoT Devices

The rapid evolution of the Internet of Things (IoT) has given rise to a wide range of devices that share several defining features. These features distinguish IoT devices from conventional embedded systems and play a crucial role in ensuring seamless connectivity, data exchange, and intelligent decision-making. Understanding these key features is essential for the design and implementation of efficient, reliable, and scalable IoT systems. The major features of IoT devices include sensing capability, connectivity, interoperability, intelligence, scalability, security, and energy efficiency.

a) Sensing Capability.: The fundamental feature of IoT devices is their ability to sense and collect real-world data through various sensors. These sensors measure physical parameters such as temperature, humidity[2], motion, pressure, or chemical concentration. The accuracy, sensitivity, and resolution of sensing components directly influence the overall system performance. Sensing capability forms the basis of IoT functionality, enabling devices to interact with their environment and provide meaningful data for analysis and automation.

b) Connectivity.: Connectivity is the backbone of IoT devices, allowing them to communicate and share data across networks. IoT devices utilize a wide range of communication technologies, including Wi-Fi, Bluetooth, Zigbee, LoRa, NB-IoT, and 5G, depending on the application and deployment scenario. Reliable connectivity ensures real-time data transfer, remote monitoring, and coordinated actions between distributed devices. The choice of communication protocol significantly affects the system's latency, bandwidth, power consumption, and scalability.

c) Interoperability.: Interoperability refers to the ability of IoT devices and systems to communicate, exchange data, and function together, regardless of manufacturer or platform differences. It is a critical feature that enables seamless integration of heterogeneous devices within a common ecosystem. Interoperability is achieved through standardized communication protocols, middleware platforms, and data formats. Lack of interoperability remains one of the major challenges in large-scale IoT deployments[11], often leading to vendor lock-in and reduced flexibility.

d) Intelligence.: Intelligence in IoT devices is realized through embedded processing and decision-making capabilities. Modern IoT systems integrate artificial intelligence (AI) and machine learning (ML) algorithms to enable context-aware responses, predictive maintenance, and automated control. Edge and fog computing further enhance device intelligence by allowing local data processing, reducing dependence on cloud infrastructure. Intelligent IoT devices can learn from user behavior, optimize operations, and adapt dynamically to environmental changes.

e) Scalability.: Scalability is a key feature that allows IoT systems to accommodate a growing number of connected devices without compromising performance. A scalable IoT architecture ensures efficient data handling, communication management, and resource allocation as the network expands. Scalability is particularly important in large-scale applications such as smart cities, industrial automation, and environmental monitoring, where thousands of devices must operate concurrently and reliably.

f) Security.: Security is a critical concern in IoT device design due to the vast amount of sensitive data transmitted over networks. Key aspects of IoT security include authentication, encryption, access control[12], and firmware integrity. Devices must be protected from cyber-attacks, unauthorized access, and data breaches[3]. Implementing lightweight security protocols suitable for resource-constrained devices remains an ongoing research challenge in the IoT domain.

g) Energy Efficiency.: Energy efficiency is an essential feature for ensuring prolonged device operation, especially for battery-powered and energy-harvesting IoT devices. Optimized power management strategies, low-power communication protocols, and sleep scheduling mechanisms help minimize energy consumption. Energy-efficient IoT devices enable sustainable deployments in remote or inaccessible locations, reducing maintenance costs and environmental impact.

h) Remote Accessibility and Control.: IoT devices are designed to be accessible and controllable remotely through the internet or mobile applications. This feature enables users and administrators to monitor system status, configure parameters, and perform maintenance from distant locations. Remote accessibility enhances convenience, reduces downtime, and enables continuous operation of critical systems such as healthcare monitoring, industrial control, and environmental observation.

i) Adaptability and Upgradability.: Adaptability allows IoT devices to function effectively in dynamic environments by adjusting to changes in network conditions, workload, or environmental factors. Upgradability, on the other hand, enables the devices to receive firmware or software updates remotely, ensuring long-term functionality and security compliance. Together, these features contribute to the resilience and longevity of IoT systems.

Overall, these key features collectively define the operational efficiency, reliability, and intelligence of IoT devices. Understanding and optimizing these characteristics are vital for the successful development and deployment of modern IoT ecosystems across various domains.

IV. Emerging Trends in IoT Devices

The landscape of IoT devices is continuously evolving, driven by advancements in hardware, software, connectivity, and data analytics. Emerging trends reflect the increasing complexity, intelligence, and integration of IoT systems across diverse application domains. Understanding these trends is essential for researchers, developers, and practitioners aiming to design next-generation IoT solutions. Key trends in IoT devices include edge and fog computing, AI and machine learning integration, low-power wide-area networks (LPWANs), wearable and implantable devices, interoperability standards, and enhanced security measures.

a) Edge and Fog Computing.: Edge and fog computing are gaining prominence as IoT systems generate massive amounts of data that cannot be efficiently processed solely in the cloud. By performing data processing and analytics closer to the source, these paradigms reduce latency, bandwidth usage, and dependence on centralized infrastructure. Edge and fog-enabled IoT devices are particularly beneficial in time-sensitive applications such as autonomous vehicles, industrial automation, and healthcare monitoring[13], [16].

b) Integration of Artificial Intelligence and Machine Learning.: IoT devices are increasingly incorporating AI and machine learning algorithms to enable intelligent decision-making, predictive analytics, and context-aware responses. This trend allows devices to learn from historical and real-time data, optimize operations, detect anomalies, and provide personalized user experiences. AI-enabled IoT devices are transforming industries such as smart homes, healthcare, agriculture, and manufacturing by automating complex processes and enhancing operational efficiency.

c) Low-Power Wide-Area Networks (LPWANs).: LPWAN technologies such as LoRa, NB-IoT, and LTE-M are emerging as key enablers for long-range, low-power IoT deployments. These networks support large-scale applications, including smart cities, agriculture, and environmental monitoring, by providing reliable connectivity with minimal energy consumption. The adoption of LPWANs allows IoT devices to operate autonomously for extended periods, particularly in remote or resource-constrained environments.

d) Wearable and Implantable IoT Devices.: The proliferation of wearable and implantable devices is transforming personal health monitoring and fitness tracking. Wearable devices, such as smart watches, fitness bands, and biosensors, continuously collect physiological data to provide real-time health insights. Implantable devices, including pacemakers and glucose monitors, enable long-term monitoring of critical health parameters. This trend underscores the growing intersection of IoT with healthcare and personalized medicine.

e) Interoperability and Standardization.: The need for seamless integration among heterogeneous IoT devices has led to an increased focus on interoperability and standardization. Emerging standards and protocols facilitate communication between devices from different manufacturers and platforms, ensuring efficient data exchange and system integration. Adoption of standardized frameworks is crucial for scalable IoT ecosystems and for minimizing issues such as vendor lock-in and compatibility challenges.

f) Enhanced Security and Privacy Measures.: As IoT devices become more pervasive, concerns regarding security, privacy, and data protection are driving the development of advanced security mechanisms. Trends include the implementation of lightweight encryption, secure authentication protocols, blockchain-based security solutions, and privacy-preserving data analytics. Ensuring robust security is essential to maintaining user trust, preventing cyberattacks, and safeguarding sensitive information in IoT networks.

g) Energy Harvesting and Sustainable Designs.: Sustainable and energy-efficient designs are emerging as a key trend in IoT device development. Devices are increasingly incorporating energy-harvesting technologies, such as solar, vibration, and thermal energy, to reduce dependency on batteries and grid power. Sustainable IoT designs support long-term deployments in remote areas, reduce operational costs, and contribute to environmentally responsible solutions.

h) Convergence with 5G and Beyond.: The integration of IoT devices with 5G networks is enabling ultra-reliable, low-latency communication and massive device connectivity. This trend supports emerging applications such as autonomous vehicles, industrial IoT, augmented reality, and remote healthcare. Future generations of wireless networks are expected to further enhance IoT capabilities, enabling even more sophisticated and real-time applications.

These emerging trends collectively indicate a shift towards more intelligent, autonomous, and connected IoT ecosystems. They highlight the potential of IoT devices to transform diverse sectors while addressing challenges related to scalability, reliability, energy efficiency, and security.

V. Challenges and Future Directions

Despite the rapid growth and adoption of IoT devices, several challenges remain that hinder their full potential. Addressing these issues is critical for creating reliable, scalable, and secure IoT ecosystems. Key challenges and future research directions include interoperability, security and privacy, energy efficiency, data management, and standardization.

a) Interoperability.: The heterogeneity of IoT devices, communication protocols, and platforms creates significant interoperability challenges. Devices from different manufacturers often face difficulties in seamless integration, limiting the scalability and flexibility of IoT systems. Future research is focusing on developing universal standards, middleware solutions, and standardized data formats to enhance device compatibility and enable cohesive IoT ecosystems.

b) Security and Privacy.: Security and privacy remain critical concerns due to the vast amounts of sensitive data transmitted and stored by IoT devices. Vulnerabilities in device firmware, communication channels, and cloud platforms can lead to cyberattacks and data breaches. Emerging solutions include lightweight encryption algorithms, secure authentication protocols, blockchain-based security mechanisms, and privacy-preserving data analytics. Ensuring robust security and compliance with privacy regulations will remain a major focus in the future development of IoT systems.

c) Energy Efficiency.: Many IoT devices are battery-powered or deployed in resource-constrained environments, making energy efficiency a persistent challenge. Advances in low-power communication protocols, energy-harvesting technologies, and optimized power management strategies are crucial for prolonging device lifespan and supporting sustainable IoT deployments.

d) Data Management and Analytics.: The exponential growth of IoT-generated data poses challenges for storage, processing, and analysis. Efficient data management frameworks, real-time analytics, and edge/fog computing architectures are required to handle large-scale data streams. Future trends include AI-driven analytics, predictive modeling, and distributed computing approaches to extract actionable insights while minimizing latency.

e) Standardization and Regulatory Compliance.: The lack of universal standards and varying regulatory requirements across regions can impede the widespread deployment of IoT devices. Standardization efforts in communication protocols, device certification, and data formats will be critical to facilitate global interoperability, compliance, and large-scale adoption of IoT solutions.

VI. Conclusion

This paper presents a comprehensive overview of modern IoT devices, focusing on their classification, key features, and emerging trends. The multidimensional classification highlights the diversity of IoT devices based on functionality, communication range, power sources, deployment environments, data processing location, and application domains. Key features such as sensing capability, connectivity, intelligence, scalability, and security define their operational efficiency and adaptability. Emerging trends, including edge and fog computing, AI integration, LPWANs, wearable devices, and sustainable designs, demonstrate the rapid evolution of IoT technologies.

While significant advancements have been achieved, challenges related to interoperability, security, energy efficiency, and data management remain. Addressing these issues through standardization, robust security measures, and innovative energy solutions will drive the next generation of IoT systems. Overall, IoT devices continue to transform smart homes, healthcare, agriculture, industrial processes, and environmental monitoring, paving the way for more intelligent, connected, and sustainable ecosystems in the future.

References

[1] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] Hudda, S., Haribabu, K. A review on WSN based resource constrained smart IoT systems. Discov Internet Things 5, 56 (2025). https://doi.org/10.1007/s43926-025-00152-2

[3] Gunjal, P.R., Jondhale, S.R., Lloret Mauri, J., & Agrawal, K. (2024). Internet of Things: Theory to Practice (1st ed.). CRC Press. https://doi.org/10.1201/9781003282945

[4] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[5] E. Borgia, “The Internet of Things vision: Key features, applications and open issues,” *Computer Communications*, vol. 54, pp. 1–31, 2014.

[6] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of Things for smart cities,” *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, 2014.

[7] S. Li, L. Da Xu, and S. Zhao, “5G Internet of Things: A survey,” *Journal of Industrial Information Integration*, vol. 10, pp. 1–10, 2018.

[8] Intersection of Artificial Intelligence, Data Science, and Cutting-Edge Technologies: From Concepts to Applications in Smart Environment, https://doi.org/10.1007/978-3-031-90921-4

[9] Khang, A., Abdullayev, V., Hahanov, V., & Shah, V. (Eds.). (2024). Advanced IoT Technologies and Applications in the Industry 4.0 Digital Economy (1st ed.). CRC Press. https://doi.org/10.1201/9781003434269

[10] Garg, U., Gupta, N., Singh, R., Gehlot, A., & Dumka, A. (2025). Anatomy of IoT Botnets and Detection Methods (1st ed.). CRC Press. https://doi.org/10.1201/9781003631460

[11] A. Antonić, M. Marjanović, P. Skočir and I. P. Žarko, ”Comparison of the CUPUS middleware and MQTT protocol for smart city services,” 2015 13th International Conference on Telecommunications (ConTEL), Graz, Austria, 2015, pp. 1-8, doi: 10.1109/ConTEL.2015.7231225.

[12] Agrawal, N., Kumar, R., & Tapaswi, S. (2025). Cloud Computing Security: Strategies and Best Practices (1st ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9781003510772

[13] Phuchortham, S., & Sabit, H. (2025). A Survey on Free-Space Optical Communication with RF Backup: Models, Simulations, Experience, Machine Learning, Challenges and Future Directions. Sensors, 25(11), 3310. https://doi.org/10.3390/s25113310

[14] Md. Hafizur Rahman, M.Naderuzzaman, “A Comprehensive Review of M2M Communication Protocols”, Open Access Journal on Engineering Applications (OAJEA), Volume No. 01, Issue No. 01, Page 1-13, July, 2025. https://doi.org/10.64886/oajea.0101.001

[15] Md. Hafizur Rahman,Dr. Zohra Khatun, M.Naderuzzaman, “A Smart IoT-Based Environmental Monitoring System for Clinical Labs: Focus on Temperature, Humidity and Air Quality”, Open Access Journal on Engineering Applications (OAJEA), Volume No. 01, Issue No. 01, Page 14-17, July, 2025. https://doi.org/10.64886/oajea.0101.002

[16] Md Hafizur Rahman “A Comprehensive Review of Edge Computing: A Perspective of IoT”, Open Access Journal on Engineering Applications (OAJEA), Volume No. 01, Issue No. 01, Page 29-37, July, 2025. https://doi.org/10.64886/oajea.0101.004

[17] Rahman, M. H., Reza, M. M., Ferdous, R., Naderuzzaman, Kashem, M. A. (2025). Development of a IoT Based Thermologger for Real-Time Temperature Monitoring. Internet of Things and Cloud Computing, 13(2), 28-37. https://doi.org/10.11648/j.iotcc.20251302.11