ISSN: 2393-8048
International Advance Journal of Engineering, Science and Management (IAJESM)
Multidisciplinary, Multilingual, Indexed, Double Blind, Open Access, Peer-Reviewed, Refereed-International Journal.
SJIF Impact Factor = 8.35, January-June 2026, Submitted in January 2026

Internet of Things (IoT): A Survey on Architectures and Protocols

Dr. Sathe Amol Kundalik, Assistant Professor, Department of Computer Science, SSPM's Chandmal Tarachand Bora Arts, Commerce and Science College, Shirur, Dist. Pune – 412210
Lembe Komal Rajendra, Post Graduate Student, Department of Computer Science, Chandmal Tarachand Bora Arts, Commerce and Science College, Shirur, Pune
Mulay Payal Shashikant, Post Graduate Student, Department of Computer Science, Chandmal Tarachand Bora Arts, Commerce and Science College, Shirur, Pune
Kothawale Omkar Shantaram, Post Graduate Student, Department of Computer Science, Chandmal Tarachand Bora Arts, Commerce and Science College, Shirur, Pune

Abstract

The Internet of Things (IoT) has emerged as one of the most transformative technologies of the modern digital era. IoT enables communication among physical devices, sensors, actuators, and software applications through internet connectivity. It integrates smart objects with communication networks to provide intelligent services in domains such as healthcare, agriculture, transportation, manufacturing, smart cities, and home automation. The rapid increase in connected devices has led to the development of various IoT architectures and communication protocols to support scalability, interoperability, energy efficiency, and security. This survey paper presents a comprehensive study of IoT architectures and communication protocols. The paper discusses layered IoT architectures, cloud and edge-based models, and analyzes major IoT communication protocols such as MQTT, CoAP, AMQP, XMPP, ZigBee, Bluetooth Low Energy (BLE), LoRaWAN, and 6LoWPAN. The study also highlights security challenges, applications, advantages, limitations, and future research directions in IoT systems. The objective of this survey is to provide researchers and students with a detailed understanding of IoT frameworks and communication technologies.

Keywords: Internet of Things, IoT Architecture, MQTT, CoAP, 6LoWPAN, ZigBee, Edge Computing, IoT Protocols, Smart Devices, Wireless Sensor Networks

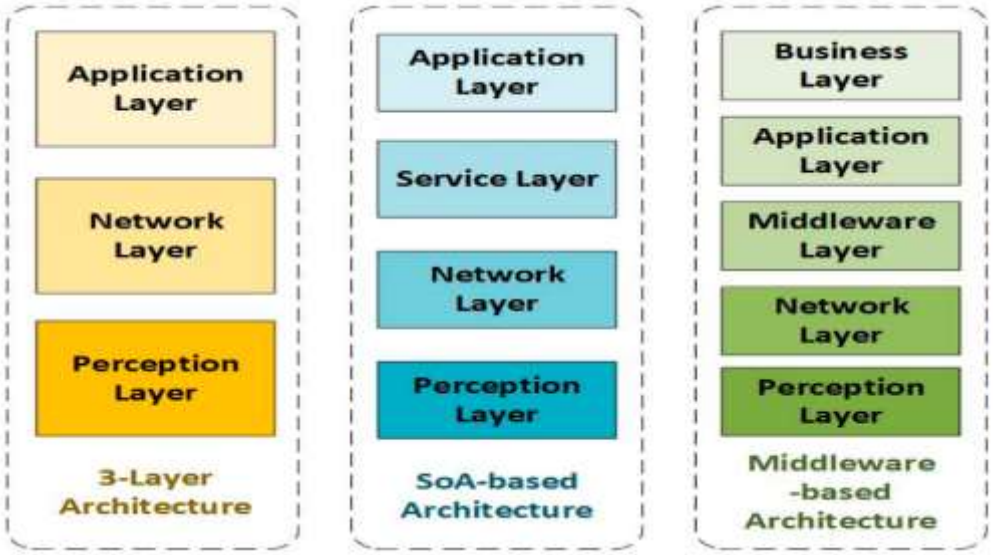
1. Introduction

The Internet of Things (IoT) refers to a network of interconnected physical devices capable of collecting, exchanging, and processing data over the internet with minimal human intervention. These devices include sensors, actuators, wearable devices, smart appliances, industrial machines, and vehicles. IoT combines several technologies such as embedded systems, wireless communication, cloud computing, artificial intelligence, and data analytics.

The concept of IoT was introduced to create intelligent communication between machines and humans. In recent years, IoT has gained significant importance due to the growth of smart devices and wireless networks. IoT systems are now used in healthcare monitoring, industrial automation, smart agriculture, smart homes, environmental monitoring, and transportation systems.

IoT architectures define how devices communicate, process data, and deliver services. Communication protocols play an essential role in ensuring reliable and efficient data transmission between devices. Since IoT devices are resource-constrained in terms of memory, battery, and processing capability, lightweight protocols are preferred.

Recent surveys highlight that protocols such as MQTT and CoAP are widely adopted due to low power consumption and efficient communication mechanisms.



2. Characteristics of IoT

The major characteristics of IoT are as follows:

1. **Connectivity:**
   Devices are connected through wired or wireless networks.
2. **Scalability:**
   IoT systems support billions of connected devices.
3. **Heterogeneity:**
   Devices differ in hardware, communication methods, and operating systems.
4. **Dynamic Nature:**
   IoT devices frequently join or leave the network.
5. **Real-Time Communication:**
   IoT enables instant monitoring and decision-making.
6. **Intelligence:**
   IoT systems use analytics and AI to automate operations.
7. **Energy Efficiency:**
   Many IoT devices operate on limited battery power.

3. IoT Architecture

IoT architecture defines the structure of IoT systems and communication among devices, networks, and applications. Different architectures have been proposed depending on system complexity and applications.

3.1 Three-Layer Architecture

The three-layer architecture is the basic model of IoT.

a) Perception Layer

- Responsible for sensing and collecting data from the environment.
- Includes sensors, RFID tags, GPS modules, and actuators.

b) Network Layer

- Transfers data from devices to servers using communication technologies such as Wi-Fi, Bluetooth, ZigBee, and cellular networks.

c) Application Layer

- Provides services to users such as healthcare monitoring, smart homes, and industrial automation.

Advantages

- Simple and easy to implement
- Suitable for small IoT systems

Limitations
- Lack of security and data management
- Limited scalability

3.2 Five-Layer Architecture

To overcome limitations of the three-layer model, a five-layer architecture was introduced.

Layers:

1. Perception Layer
2. Transport Layer
3. Processing Layer
4. Application Layer
5. Business Layer

Features
- Better data processing
- Improved management and security
- Supports cloud computing and analytics

3.3 Cloud-Based IoT Architecture

Cloud computing plays a major role in IoT by providing:
- Large storage capacity
- Data analytics
- Remote access
- Scalability

In cloud-based architecture:
- IoT devices send data to cloud servers.
- Cloud platforms process and analyze data.
- Users access services through web or mobile applications.

Advantages
- High scalability
- Centralized data management
- Cost efficiency

Limitations
- High latency
- Internet dependency
- Privacy concerns

Cloud, edge, and fog-based IoT architectures are commonly discussed in recent IoT surveys.

3.4 Edge and Fog Computing Architecture

Edge Computing

Data processing occurs near IoT devices instead of centralized cloud servers.

Fog Computing

Fog nodes are placed between cloud and edge devices to reduce latency.

Benefits
- Reduced response time
- Lower bandwidth usage
- Enhanced real-time processing

Applications
- Autonomous vehicles
- Smart traffic systems
- Industrial automation

4. IoT Communication Protocols

Communication protocols define rules for data transmission among IoT devices. Protocols are categorized according to IoT layers.

5. Application Layer Protocols

5.1 MQTT (Message Queuing Telemetry Transport)

MQTT is a lightweight publish-subscribe messaging protocol designed for low-bandwidth and constrained devices.

Features

- Low power consumption
- Small packet size
- Reliable communication
- Broker-based architecture

Working

- Publisher sends messages to a broker.
- Subscribers receive messages from the broker.

Advantages

- Efficient for remote monitoring
- Supports Quality of Service (QoS)

Limitations

- Requires continuous TCP connection
- Broker dependency

MQTT is one of the most widely used protocols in IoT systems.

5.2 CoAP (Constrained Application Protocol)

CoAP is a lightweight protocol designed for constrained devices and low-power networks.

Features

- Based on UDP
- Low overhead
- Request-response model
- RESTful architecture

Advantages

- Faster communication
- Suitable for low-power devices

Limitations

- Less reliable than TCP-based protocols

Research comparing CoAP and MQTT shows CoAP performs efficiently in constrained IP-based networks.

5.3 AMQP (Advanced Message Queuing Protocol)

AMQP is a reliable messaging protocol mainly used in enterprise applications.

Features

- Secure communication
- Message orientation
- Reliable delivery

Applications

- Financial systems
- Enterprise IoT

Limitation

- Higher complexity compared to MQTT

5.4 XMPP (Extensible Messaging and Presence Protocol)

XMPP is an XML-based communication protocol.

Features

- Real-time communication
- Secure messaging
- Interoperability

Applications
- Smart homes
- Instant messaging systems

Limitation
- High bandwidth usage due to XML formatting

6. Network Layer Protocols

6.1 6LoWPAN

6LoWPAN enables IPv6 communication over low-power wireless networks.

Features
- IPv6 support
- Low energy consumption
- Small packet size

Applications
- Wireless sensor networks
- Smart homes

6.2 RPL (Routing Protocol for Low-Power and Lossy Networks)

RPL is designed for routing in constrained IoT networks.

Features
- Energy-efficient routing
- Supports large-scale networks

Applications
- Industrial IoT
- Smart agriculture

7. Data Link and Physical Layer Protocols

7.1 ZigBee

ZigBee is a low-power wireless communication technology based on IEEE 802.15.4.

Features
- Low energy usage
- Mesh networking
- Short-range communication

Applications
- Home automation
- Smart lighting

7.2 Bluetooth Low Energy (BLE)

BLE is designed for short-range wireless communication with low power consumption.

Applications
- Wearable devices
- Healthcare monitoring

Advantages
- Energy efficient
- Low cost

7.3 LoRaWAN

LoRaWAN supports long-range communication for low-power devices.

Features
- Long communication range
- Low battery usage
- Suitable for remote areas

Applications
- Smart agriculture
- Environmental monitoring

7.4 NB-IoT

NB-IoT is a cellular-based LPWAN technology.

Features

- Wide coverage
- Low power consumption
- Massive device connectivity

Applications

- Smart metering
- Industrial automation

8. Comparison of IoT Protocols

Protocol	Layer	Transport	Power Consumption	Communication Model	Applications
MQTT	Application	TCP	Low	Publish-Subscribe	Smart Homes
CoAP	Application	UDP	Very Low	Request-Response	Sensor Networks
AMQP	Application	TCP	Medium	Message-Oriented	Enterprise Systems
XMPP	Application	TCP	High	Messaging	Chat Applications
ZigBee	Data Link	IEEE 802.15.4	Low	Mesh	Home Automation
BLE	Data Link	Bluetooth	Very Low	Point-to-Point	Wearables
LoRaWAN	Network	LPWAN	Very Low	Long-Range	Smart Agriculture

Protocol classifications and IoT stack mappings are widely discussed in IoT literature.

9. IoT Security Challenges

Security is one of the major concerns in IoT systems due to limited device resources and heterogeneous environments.

Major Challenges

1. Data Privacy

Sensitive information may be exposed during transmission.

2. Authentication

Unauthorized devices can access networks.

3. Data Integrity

Attackers may modify transmitted data.

4. Malware Attacks

IoT devices are vulnerable to botnets and malware.

5. Denial of Service (DoS)

Attackers overload devices or servers.

Authentication and security protocols remain active research areas in IoT.

10. Applications of IoT

10.1 Smart Healthcare

- Remote patient monitoring
- Wearable devices
- Smart medical equipment

10.2 Smart Agriculture

- Soil monitoring
- Automated irrigation
- Crop health monitoring

10.3 Smart Cities
- Smart traffic management
- Waste management
- Energy-efficient lighting

10.4 Industrial IoT
- Predictive maintenance
- Industrial automation
- Supply chain management

10.5 Smart Homes
- Smart lighting
- Smart security systems
- Voice-controlled appliances

11. Advantages of IoT
- Automation and efficiency
- Real-time monitoring
- Reduced human effort
- Better resource management
- Enhanced decision-making

12. Limitations of IoT
- Security vulnerabilities
- High implementation cost
- Privacy issues
- Complexity in interoperability
- Dependence on internet connectivity

13. Future Directions of IoT

Future IoT research focuses on:
- Artificial Intelligence integration
- 5G-enabled IoT
- Blockchain for security
- Green IoT
- Edge AI systems
- Quantum communication for IoT security

Emerging studies also emphasize edge and fog computing architectures to reduce latency and improve scalability.

14. Conclusion

The Internet of Things has become an essential technology for smart environments and intelligent automation. IoT architectures provide structured frameworks for communication, processing, and service delivery, while communication protocols ensure efficient and reliable data transmission among constrained devices. Protocols such as MQTT, CoAP, ZigBee, BLE, and LoRaWAN have gained significant importance due to their lightweight and energy-efficient nature. However, security, scalability, interoperability, and privacy remain major challenges in IoT deployment. Future advancements integrating AI, 5G, edge computing, and blockchain are expected to improve IoT performance and security. This survey provides a detailed overview of IoT architectures and protocols that can assist researchers, students, and practitioners in understanding current developments and future trends in IoT systems.

References

1. Tara Salman and Raj Jain, "A Survey of Protocols and Standards for Internet of Things," IEEE Communications Surveys & Tutorials, 2019.
2. Abdulkadir Dauda, Olivier Flauzac, Florent Nolot, "A Survey on IoT Application Architectures," Sensors Journal, 2024.

3. Mishra B., Kertész A., "The Use of MQTT in M2M and IoT Systems: A Survey," IEEE Access, 2020.
4. "Transport and Application Layer Protocols for IoT: Comprehensive Review," Technologies Journal, 2025.
5. "Internet of Things: A General Overview between Architectures, Protocols and Applications," Information Journal, 2021.
6. "A survey on communication protocols and performance evaluations for Internet of Things," Digital Communications and Networks, 2022.
7. "A–Z Survey of Internet of Things: Architectures, Protocols, Applications, Recent Advances, Future Directions and Recommendations," Journal of Network and Computer Applications, 2020.
8. Cenk Gündoğan et al., "NDN, CoAP, and MQTT: A Comparative Measurement Study in the IoT," 2018.
9. Mohamed Amine Ferrag et al., "Authentication Protocols for Internet of Things: A Comprehensive Survey," 2016.
10. "A Survey of Communication Protocols in IoT: MQTT, CoAP, and Beyond," International Journal of Computer Technology and Electronics Communication, 2025.