

Wireless Sensor Networks in IoT: Architecture, Applications, Challenges and Future Directions

Shraddha Raghunath Hande¹, Prajakta Sanjay Badhekar², Vaishnavi Adinath Chavare³

Department of Information Technology

Government Polytechnic Awasari Khurd, Awasari Khurd, Pune, Maharashtra, India

Author email addresses: shraddha.hande@gmail.com;

prajaktabadhekar@gmail.com; vaishnavi.chavare2008@gmail.com

Abstract: *Wireless Sensor Networks (WSNs) are an important enabling technology for the Internet of Things (IoT). A WSN consists of distributed sensor nodes that collect information from physical environments and communicate the collected data through wireless links to a sink, gateway, or IoT platform. This review paper discusses the basic architecture of WSN-enabled IoT systems, the main components of sensor nodes, commonly used communication technologies, application areas, and major implementation challenges. The review is based on published literature rather than a new hardware implementation or experimental evaluation. The literature indicates that energy consumption, network lifetime, communication reliability, interoperability, security, privacy, and deployment conditions remain important considerations when designing WSN-based IoT solutions. Applications include environmental monitoring, precision agriculture, healthcare, industrial monitoring, smart buildings, and smart cities. The paper summarizes design considerations and identifies directions such as energy-aware networking, edge processing, stronger device security, and integration with emerging connectivity technologies. The discussion is intended to provide an introductory technical overview for students and readers studying WSN and IoT systems.*

Keywords: Wireless Sensor Network, Internet of Things, Sensor Node, Energy Efficiency, IoT Communication, Network Security

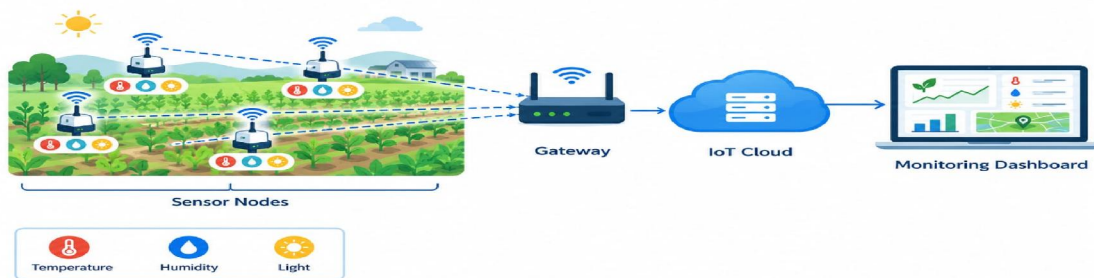
I. INTRODUCTION

The Internet of Things (IoT) connects physical objects equipped with sensing, processing, and communication capabilities so that information can be collected, exchanged, and used by applications. Wireless Sensor Networks (WSNs) support this model by allowing multiple sensor nodes to monitor physical conditions and forward measurements over wireless links. Depending on the application, a node may measure temperature, humidity, pressure, light, vibration, motion, or other parameters. The collected information can help users observe conditions remotely and make informed decisions [1], [2].

A typical WSN-enabled IoT system includes sensor nodes, a wireless communication network, a sink or gateway, an Internet connection, a data-processing platform, and a user application. Not every deployment uses the same arrangement: some systems communicate directly with a gateway, while others forward data through multiple nodes or use low-power wide-area network technologies. The design depends on coverage, data rate, latency, power availability, cost, and the environment in which the nodes operate [1], [3].

This paper reviews the architecture, components, communication options, application domains, and key challenges of WSNs in IoT. It is a literature-based review and does not claim to present new experiments, measurements, or prototype results.





II. REVIEW METHODOLOGY

This paper uses a narrative literature-review approach. Relevant published review articles and research papers on WSN architecture, IoT protocols, sensor applications, energy optimization, and security challenges were consulted. Sources were selected for their direct relevance to WSN-enabled IoT systems and for providing technical discussion of architecture, applications, or open problems. The review synthesizes the themes discussed in those sources; it is not a systematic review and does not claim exhaustive coverage of every publication in the field.

III. ARCHITECTURE OF WSN-BASED IoT

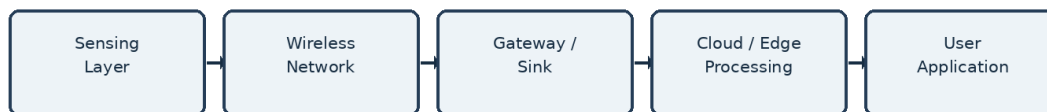


Fig. 1. WSN-Based IoT Architecture

A WSN-based IoT architecture can be described using the following functional components:

A. Sensing Layer: Sensor elements measure physical or environmental conditions. A microcontroller or embedded processor may filter, format, or locally process the measurements.

B. Communication Layer: A radio module transfers readings to nearby nodes, a sink, or a gateway. Depending on the use case, technologies may include IEEE 802.15.4-based networks, Bluetooth Low Energy, Wi-Fi, LoRaWAN, or cellular IoT. Their range, throughput, power use, and infrastructure requirements differ.

C. Gateway or Sink: The gateway gathers data from sensor nodes and may translate protocols, buffer information, perform basic filtering, and forward data to an IP network or cloud service.

D. Processing and Storage Layer: Edge devices or cloud platforms store, aggregate, visualize, and analyse sensor data. Processing close to the sensors can reduce response time and unnecessary network traffic.

E. Application Layer: A user-facing application displays readings, sends alerts, produces reports, or supports monitoring and control decisions.

These layers are a conceptual model rather than a single mandatory standard. Actual deployments may combine or separate functions according to requirements. IoT architecture and protocol choices are discussed broadly in [2], [3].



IV. COMPONENTS OF A SENSOR NODE



Fig. 2. Basic Components of a Sensor Node

A sensor node commonly contains a sensing unit, a processing unit, a wireless transceiver, and a power source. The sensing unit converts a physical condition into a signal. The processing unit manages sampling, simple computation, and communication tasks. The transceiver sends and receives packets, while the battery or other energy source powers the node. Some devices also include memory, positioning capability, actuators, or energy-harvesting components. Since many nodes have limited battery capacity and memory, the choice of sampling frequency, radio duty cycle, and local processing can affect operational lifetime [1], [4].

V. COMMUNICATION TECHNOLOGIES

No single wireless technology is suitable for every IoT sensor deployment. Short-range technologies can be appropriate for homes, buildings, and personal-area applications, whereas low-power wide-area technologies can support small messages over longer distances. Wi-Fi can offer higher data rates but may require more energy than some low-power alternatives. Bluetooth Low Energy is often used for short-range, low-power links. IEEE 802.15.4-based technologies support low-rate wireless personal area networking, while LoRaWAN and cellular IoT options address different wide-area connectivity needs. Technology selection should consider coverage, battery life, data volume, latency, interference, security support, deployment cost, and available infrastructure [2], [3].

VI. APPLICATIONS OF WSN IN IoT

A. Environmental Monitoring: Sensor nodes can monitor temperature, humidity, air quality, water quality, or other environmental indicators. Measurements can help identify changes over time and support timely alerts.

B. Precision Agriculture: Soil-moisture, temperature, and humidity sensors can provide information to support irrigation scheduling and crop-condition monitoring. The usefulness of such systems depends on sensor placement, connectivity, calibration, and field conditions.

C. Healthcare and Wearable Monitoring: Wireless sensors can collect selected physiological or activity-related measurements and transmit them to monitoring systems. Medical applications require careful attention to accuracy, privacy, reliability, and applicable regulations.

D. Industrial Monitoring: Sensors can observe vibration, temperature, pressure, or machine operating conditions. These data can support condition monitoring and maintenance planning, although industrial systems may require strict reliability and security controls.

E. Smart Buildings and Smart Cities: WSNs can support occupancy sensing, lighting control, utility monitoring, waste management, and infrastructure observation. The design must address scale, device management, and protection against unauthorized access.

The literature describes a wide range of WSN and IoT applications, while also noting that deployment requirements vary substantially across environments [1], [2], [5].

VII. KEY CHALLENGES

A. Energy Consumption and Network Lifetime: Wireless communication and repeated sensing consume energy. Replacing batteries can be difficult when nodes are numerous or installed in inaccessible locations. Energy-aware



routing, duty cycling, efficient sampling, and data aggregation are common approaches discussed in the literature [4], [6].

B. Communication Reliability and Coverage: Obstacles, interference, distance, node failure, and changing environmental conditions can reduce packet delivery or create coverage gaps. Network planning and suitable link technologies are therefore important.

C. Security and Privacy: Sensor data and device controls may be exposed to eavesdropping, spoofing, unauthorized access, or tampering if protection is weak. Authentication, encryption, secure updates, access control, and careful key management are important design considerations.

D. Interoperability and Scalability: Devices from different manufacturers may use different protocols, data formats, and management systems. Integration and large-scale device administration can increase complexity.

E. Cost and Maintenance: Hardware, connectivity, calibration, gateway infrastructure, and long-term maintenance all affect the total cost. Environmental conditions may also shorten sensor or battery life.

These challenges are interdependent. For example, stronger security can add processing and communication overhead, while energy-saving settings may affect latency or responsiveness. Designers must balance requirements according to the application [1], [4], [6].

VIII. FUTURE DIRECTIONS

Several directions may improve future WSN-enabled IoT deployments. Energy harvesting may reduce dependence on battery replacement in suitable environments, although harvested energy can be variable. Edge computing can process data near the source and may reduce unnecessary transmission. Machine-learning methods may help detect unusual sensor patterns or support predictive maintenance when sufficient high-quality data and computing resources are available. Improved device identity, secure provisioning, authenticated updates, and lifecycle management can strengthen security. Finally, integration across different low-power and wide-area communication technologies may help systems match connectivity to application requirements. These are potential directions discussed in the broader literature, not results demonstrated by this paper [1], [2], [4].

IX. DISCUSSION

The reviewed literature shows that WSNs provide a practical sensing foundation for many IoT applications, but successful deployment requires more than selecting a sensor and radio. Architecture, energy budget, network topology, communication protocol, data processing, security, and maintenance should be considered together. A low-power environmental monitoring node may prioritize long battery life and modest data rates, while an industrial monitoring system may place greater emphasis on reliability, latency, and secure operation. Therefore, technology selection should follow the needs of the application rather than assuming that one architecture or protocol is universally best.

Detailed Architecture and Data Flow

A WSN-enabled IoT system can be understood as a sequence of sensing, local processing, communication, gateway handling, and application-level analysis. At the sensing stage, each node measures a physical condition such as temperature, humidity, light intensity, vibration, soil moisture, or air quality. The node converts the physical signal into a digital reading through a sensor interface and analog-to-digital conversion where required. A microcontroller may then filter noise, check whether the reading is within a plausible range, attach a timestamp or node identifier, and prepare a packet for transmission.

The communication stage transfers the packet to a neighbouring node, a cluster head, or a gateway. In a multi-hop network, intermediate nodes forward packets until they reach a gateway. This can extend coverage beyond the direct radio range of a single sensor, but it also creates additional forwarding work and energy use. A gateway connects the sensor network to an IP network or cloud service. Depending on the design, it may translate protocols, buffer data during temporary disconnections, apply basic rules, and send selected readings to an application server.



At the application stage, stored measurements are displayed as charts, alerts, maps, or reports. An application can compare readings with a threshold, identify a changing pattern, or notify a user that an abnormal condition has been detected. The quality of the final decision depends on the complete chain: sensor calibration, packet delivery, timestamp accuracy, data processing, and the correctness of the application rule. A reliable IoT solution therefore needs coordinated design across hardware, networking, software, and data management.

Network Topologies and Deployment Choices



Fig. 3. Illustrative WSN Network Communication

The topology describes how sensor nodes are connected. In a star topology, each sensor communicates directly with a central gateway or coordinator. This design is simple to manage and can reduce forwarding overhead, but nodes outside the gateway's radio range may not be able to participate. A tree topology organizes nodes in parent-child relationships. It can cover a larger area, although a failure near the root may affect many downstream nodes. A mesh topology permits multiple possible paths between nodes. Route alternatives can improve resilience, but maintaining routes and forwarding packets can consume extra memory, processing time, and energy.

The suitable topology depends on deployment scale, physical obstacles, radio conditions, maintenance access, and the cost of node replacement. For example, a small room-monitoring application may use a star network, whereas a large agricultural field may need multi-hop communication or multiple gateways. Industrial sites may require careful placement because metal structures and machinery can affect radio propagation. Designers should conduct a site survey, estimate the required coverage, identify likely interference sources, and allow for future expansion rather than choosing a topology based only on theoretical range.

Energy Efficiency and Network Lifetime



Fig. 4. Energy-Aware Sensor Operation

Energy is one of the most important constraints in WSN design because many sensor nodes operate on batteries and may be installed in locations that are difficult to reach. Radio transmission and reception can consume a significant part of a node's energy budget. Repeated sensing, unnecessary packet forwarding, idle listening, and retransmissions can shorten operating life. Energy-aware design aims to deliver useful information while reducing avoidable activity.

Common approaches include duty cycling, in which a node sleeps when it does not need to sense or communicate; data aggregation, in which related readings are combined before transmission; and adaptive sampling, in which the sampling rate changes according to application needs. Clustering can group nodes and assign a cluster head to collect and forward data. However, a cluster head may use more energy than ordinary nodes, so the role can be rotated or selected using energy level, distance, and traffic load. Routing protocols can also consider residual battery energy and link quality instead of selecting paths only by distance.

There is no single best energy-saving method for every application. A safety-monitoring system may require immediate alerts and cannot tolerate long sleep intervals. Environmental monitoring may accept periodic reporting and can use longer intervals during stable conditions. Energy optimization should therefore be evaluated together with latency, reliability, sensing accuracy, and the importance of the information being collected.



Communication Technologies and Protocol Selection

Wireless technologies used with WSNs differ in range, data rate, power consumption, topology, cost, and ecosystem support. IEEE 802.15.4-based technologies are designed for low-power, low-rate personal-area networking and are used by several IoT protocols. Zigbee provides networking and application features for suitable low-power mesh deployments. Bluetooth Low Energy is often appropriate for short-range devices and phone-connected sensors. Wi-Fi offers higher throughput and direct connectivity to common IP networks, but its energy demand may be unsuitable for very small battery-operated nodes unless the device can recharge frequently.

LoRaWAN is designed for long-range, low-data-rate communication and can be useful when sensors are spread across farms or remote areas. Its low throughput and duty-cycle or regional regulatory limits make it unsuitable for continuous high-volume data. Cellular IoT options can provide wide-area coverage where supported, but their modules, subscription costs, and coverage conditions need to be considered. Selection must be based on the real application rather than assuming that one technology is universally superior.

Application protocols also matter. MQTT uses a publish-subscribe model and is commonly used to transfer IoT messages through a broker. CoAP is designed for constrained devices and follows a web-like request-response approach over lightweight transport. HTTP is widely supported but can introduce more overhead for small, frequent sensor messages. A practical system may use one technology for local sensor communication and another protocol for gateway-to-cloud transfer. The gateway can bridge these layers while maintaining authentication and data integrity.

Data Quality, Storage, and Analytics

Sensor data is only useful when its meaning and quality are understood. Readings may be inaccurate because of poor calibration, sensor aging, placement, environmental interference, or hardware faults. Communication loss can create missing values, while clock differences can make readings difficult to compare. A system should record units, node identifiers, timestamps, and relevant metadata such as location or sensor type. Calibration records and maintenance history can help explain changes that appear in the data.

Basic preprocessing may remove duplicate packets, identify missing values, apply reasonable range checks, and flag abrupt changes for review. It is important not to remove unusual values automatically, because an extreme reading may represent a genuine emergency. Data should be labelled as measured, estimated, missing, or suspicious when appropriate. For long-term monitoring, storage policies should specify how raw readings, summarized values, and event records are retained.

Analytics can range from simple threshold rules to statistical methods and machine-learning models. A threshold alert is easy to explain and can work well when a clear operating limit exists. Trend analysis can help detect gradual changes, while predictive models may estimate future conditions from historical data. Such models need representative training data and ongoing evaluation. The presence of AI does not automatically make a WSN-based IoT system accurate; the model must be validated for the environment in which it is used, and the system should provide a safe fallback when data are incomplete or the model is uncertain.

Security, Privacy, and Trust

A WSN-based IoT system may be physically accessible to an attacker, especially when nodes are deployed outdoors or in public spaces. Threats can include unauthorized access, eavesdropping, replay of old messages, packet modification, denial of service, and capture of a sensor node. A compromised node may report false measurements or waste network resources. Security must therefore be considered from initial design through installation, operation, and retirement. Useful safeguards include device identity, authenticated communication, encryption where feasible, secure key provisioning, access control, signed firmware updates, and removal of default passwords. Gateways should restrict administrative access and record relevant security events. Devices should use unique credentials rather than sharing one secret across an entire deployment. Because constrained nodes have limited memory and processing capacity, cryptographic and protocol choices must be tested on the actual hardware. Lightweight design should not be interpreted as a reason to omit authentication.



Privacy depends on what is sensed and how the information is used. Environmental measurements may appear non-personal, but occupancy, location, and activity patterns can reveal sensitive information. Data minimization, limited retention, role-based access, and clear user communication can reduce risk. For critical applications, systems should also consider resilience: local alarms or safe operating modes may be necessary when the gateway or cloud service becomes unavailable.

Application Case Examples

In precision agriculture, soil-moisture and temperature sensors can help farmers understand variation across a field and schedule irrigation more carefully. A gateway can collect readings from distributed nodes and forward summaries to a dashboard. The system should account for sensor placement, changing soil conditions, network coverage, and seasonal maintenance. Recommendations should support, rather than blindly replace, agricultural knowledge and local conditions.

In smart buildings, temperature, humidity, light, and air-quality sensors can help manage ventilation, lighting, and energy use. Reporting intervals may be adjusted according to occupancy or changes in readings. Security and privacy are especially important if sensor data can reveal when people are present. In industrial monitoring, vibration and temperature measurements may indicate equipment deterioration. These applications may require higher sampling rates and low-latency alerts, so energy-saving sleep schedules must be selected carefully.

For environmental monitoring, WSN nodes can measure air quality, water conditions, weather, or forest microclimates. Long distances and limited maintenance access make energy efficiency and remote fault detection important. In healthcare-related monitoring, sensor networks can support collection of physiological or room-condition data, but accuracy, privacy, reliability, and regulatory requirements become particularly important. These examples demonstrate that the same basic WSN architecture can support many sectors, while application requirements determine the appropriate sensors, network, security, and data-processing strategy.

Implementation and Evaluation Considerations

A practical implementation should begin with requirements rather than hardware selection. The requirements should identify the variables to measure, acceptable error, reporting frequency, coverage area, maximum response delay, expected battery life, budget, and consequences of missing data. A prototype can then be used to test sensing accuracy, communication range, packet delivery, power use, and gateway integration. Testing should include realistic obstacles and interference, not only an open laboratory environment.

Useful evaluation measures include packet delivery ratio, end-to-end delay, energy consumption, network lifetime, coverage, scalability, and data accuracy. Security testing should check authentication, access control, update mechanisms, and recovery from a compromised or unavailable component. Reliability testing should include node failure, gateway disconnection, low battery, and temporary loss of internet access. Results should state the test environment and assumptions so that readers can interpret them correctly.

This paper is a literature-based review and does not report a newly built prototype or original experimental measurements. Therefore, no numerical performance claim is made here. A future student project could implement a small sensor-to-dashboard demonstration and report measured results, but those results would need to be collected, documented, and compared under defined conditions before inclusion in a research paper.

Research Gaps and Future Directions

Several continuing challenges provide opportunities for further work. First, energy-efficient operation must be balanced with fast and dependable delivery, particularly for systems that generate urgent alerts. Second, heterogeneous devices and protocols need practical interoperability so that sensors from different vendors can work together. Third, security mechanisms must remain manageable on constrained devices and across large deployments. Fourth, reliable data analytics require attention to missing readings, sensor drift, changing environments, and model explain ability. Edge computing is a promising direction because selected processing can occur near the sensor or gateway. This may reduce cloud traffic and response time, while allowing some functions to continue during internet outages. Artificial intelligence can assist with anomaly detection, predictive maintenance, and adaptive sampling, but models must be



assessed for energy cost, data requirements, false alarms, and robustness. Newer wide-area and low-power communication options may improve connectivity for remote deployments, although their suitability remains dependent on coverage, regulation, cost, and application needs.

Future research should use reproducible evaluation methods and clearly state hardware, software, topology, radio settings, workload, and environmental conditions. Comparisons should include not only average performance but also failure cases and trade-offs. Sustainable design should consider battery replacement, reparability, electronic waste, and the full lifecycle cost of deployment. These directions can help move WSN-based IoT systems from small demonstrations to dependable long-term services.

X. CONCLUSION

Wireless Sensor Networks are an important part of IoT systems because they enable distributed collection of data from the physical world. This review has summarized the functional architecture, sensor-node components, communication options, application areas, and major challenges of WSN-enabled IoT. Energy limitations, reliable communication, security, interoperability, and maintenance remain central design concerns. Energy-aware networking, edge processing, secure device management, and flexible connectivity are relevant areas for continued development. As this paper is based on existing literature, no new experimental results are claimed. Future work could compare specific technologies or evaluate a defined sensor-network prototype using clearly stated metrics and repeatable methods.

ACKNOWLEDGMENT

The authors may add an acknowledgment here if guidance, facilities, or other support was provided and the relevant person or institution has agreed to be acknowledged. This section should be removed if no acknowledgment is required.

REFERENCES

- [1] M. A. Jamshed, K. Ali, Q. H. Abbasi, M. A. Imran, and M. Ur-Rehman, "Challenges, applications and future of wireless sensors in Internet of Things: a review," *IEEE Sensors Journal*, vol. 22, no. 6, pp. 5482–5494, 2022, doi: 10.1109/JSEN.2022.3148128.
- [2] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *Journal of Electrical and Computer Engineering*, vol. 2017, Article ID 9324035, 2017, doi: 10.1155/2017/9324035.
- [3] W. Kassab and K. A. Darabkh, "A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations," *Journal of Network and Computer Applications*, vol. 163, Article 102663, 2020, doi: 10.1016/j.jnca.2020.102663.
- [4] P. Prasad et al., "Energy Optimization-Based Clustering Protocols in Wireless Sensor Networks and Internet of Things—Survey," *International Journal of Distributed Sensor Networks*, vol. 2023, Article ID 1362417, 2023, doi: 10.1155/2023/1362417.
- [5] "A survey on wireless sensor network (applications and architecture)," *International Journal of Communication Networks and Distributed Systems*, vol. 30, no. 2, pp. 136–201, 2024, doi: 10.1504/IJCND.2024.137085.
- [6] "WSN Protocols and Security Challenges for Environmental Monitoring Applications: A Survey," *Journal of Sensors*, vol. 2022, Article ID 1628537, 2022, doi: 10.1155/2022/1628537.

