Medical Management Advances 2025 1(2):1-6
https://www.auberpublishing.com/index.php/MMA/index
E-mail: editorialoffice@auberpublishing.com

Review

Application and optimization strategies of Internet of Things (IoT) technology in medical device management

Binru Zhou*

Urban Community Health Service Center, Nanda Street Sub-district, Changzhou City, Changzhou 213000, Jiangsu Province, China.

Abstract
As the healthcare industry accelerates its shift toward intelligent systems, the management of medical devices — being a critical link in this transformation — must overcome the limitations of traditional approaches. Conventional management relies heavily on manual record-keeping and periodic inspections, often resulting in delayed maintenance and inefficient resource allocation due to information lag. This paper provides an in-depth analysis of how Internet of Things (IoT) technologies can be applied to medical device management — specifically through functions such as real-time equipment monitoring and tracking, remote management and maintenance, and data collection and analysis — and explores the ways in which these applications enhance operational efficiency and device reliability. We then identify key challenges in the practical implementation of IoT — such as data security risks and device-compatibility issues — and propose targeted optimization strategies. Our goal is to offer healthcare institutions a reference framework for building safer, more efficient, and fully intelligent device-management systems.

Keywords: Internet of Things; medical device management; current applications; optimization strategies

1 Introduction

Efficient management of medical devices is fundamental to diagnostic and treatment quality and to patient safety. Under traditional management regimes, hospitals typically face two principal challenges. First, device status cannot be monitored in real time, so faults are detected belatedly, and repair cycles are lengthy — potentially delaying critical care. Second, usage information is fragmented, leading to suboptimal resource allocation: some devices remain idle for long periods while others are over-utilized. Such problems are particularly pronounced in large, complex healthcare facilities with a diverse array of equipment.

By integrating medical devices into a networked environment, IoT technology enables managers to obtain real-time operational data — temperature, usage frequency, and more — and to apply predictive algorithms to anticipate failures and schedule maintenance proactively. Furthermore, the system can analyze usage patterns to optimize device allocation and reduce idle capacity. However, real-world deployment presents hurdles: heterogeneous device-brand compatibility, protection of sensitive medical data, and other barriers must be addressed. Thus, a thorough investigation of IoT applications and their optimization strategies in medical device management carries significant practical value.

2 Overview of IoT Technology

2.1 Definition of IoT Technology

The Internet of Things leverages a variety of data-acquisition devices and techniques — sensors, radio-frequency identification (RFID), global positioning systems (GPS), infrared detectors, laser scanners, etc. — to collect real-time data from objects or processes requiring monitoring, connection, or interaction [1]. These data are

***Correspondence**
Binru Zhou
Urban Community Health Service Center, Nanda Street Sub-district, Changzhou City, Changzhou 213000, Jiangsu Province, China.
E-mail: 474972743@qq.com

then transmitted via diverse networks to establish broad interconnections among objects and between objects and people. IoT thus enables intelligent perception, precise identification, and efficient management of items and processes. In essence, it grants objects the ability to "speak," achieving seamless information sharing across networks and facilitating intelligent control and operation.

2.2 IoT Architecture

IoT systems are generally structured in three layers: the perception layer, the network layer, and the application layer [2].

a) Perception Layer

The foundational layer of IoT, its primary role is data acquisition and recognition. It integrates various sensors, RFID tags, cameras, and other devices to capture diverse environmental parameters — temperature, humidity, pressure, location, imagery, etc. In medical device management, perception-layer elements are attached directly to equipment to monitor and record operational parameters and status metrics in real time.

b) Network Layer

Acting as the data-transmission channel, the network layer employs wired technologies (Ethernet) and wireless protocols (Wi-Fi, Bluetooth, ZigBee, 4G/5G) to relay perception-layer data efficiently to cloud platforms or other processing hubs. Selection of specific communication technologies depends on coverage requirements, bandwidth needs, and cost considerations. In a medical context, the network layer must guarantee reliable and secure transmission so that device information reaches management platforms promptly and accurately.

c) Application Layer

As the core of the IoT system, the application layer aggregates, analyzes, and processes collected data to deliver decision support and tailored services for various use cases. In medical device management, application-layer development can yield systems for equipment monitoring, remote maintenance, and inventory management — empowering administrators to execute comprehensive oversight and optimized configuration of medical devices.

3 Specific Applications of IoT in Medical Device Management

3.1 Equipment Monitoring and Tracking

a) Real-Time Status Monitoring

By embedding sensors and intelligent chips in medical devices, IoT enables continuous, multi-dimensional monitoring of device operation, maintenance needs, and location. In large hospitals, where equipment is both plentiful and dispersed, manual inspection is laborious and prone to omissions. IoT platforms allow managers to view live operating parameters — voltage, current, power, etc. — for high-frequency devices such as electrosurgical units [3]. When anomalies are detected, the system triggers alerts, prompting timely intervention to prevent surgery delays or risks arising from equipment failure.

b) Device Localization and Tracking

Integrating GPS modules or indoor positioning tags into devices lets hospitals pinpoint their real-time locations. When a department urgently requires, for example, a ventilator, staff can locate and reallocate idle units rapidly, markedly improving utilization rates. For high-value equipment — MRI or CT scanners — tracking also deters theft or misplacement, safeguarding institutional assets.

3.2 Remote Management and Maintenance

a) Remote Fault Diagnosis

IoT transcends geographic constraints, enabling remote management and maintenance of medical devices [4]. In decentralized healthcare networks, especially in rural or under-resourced settings, servicing equipment is a longstanding challenge. Through IoT, technicians can monitor devices from afar and, upon detecting a fault, perform remote diagnostics. For instance, when a CT scanner in a community hospital malfunctions, engineers can analyze logs and operational data remotely, identify a software module error, and apply a corrective update — thereby averting prolonged downtime and ensuring uninterrupted patient care.

b) Preventive Maintenance

Leveraging device-health data collected via IoT and applying analytical algorithms, engineers can evaluate overall equipment condition and predict potential failures. Proactive maintenance plans are then devised to service devices before breakdowns occur, extending service life and reducing fault incidence [5]. For example, IoT sensors on hospital elevators continuously monitor parameters such as speed, vibration, and temperature; machine-learning analyses of these data can forecast issues — worn cables or motor anomalies — allowing timely dispatch of maintenance crews and preventing operational disruptions that affect patient mobility.

c) Remote Software Updates

As medical technology evolves, device software must be updated periodically to enhance performance or introduce new features. IoT integration permits technicians to push firmware upgrades remotely, obviating on-site visits and significantly cutting time and cost. For example, when a patient monitor requires a software upgrade to enable advanced monitoring capabilities, technicians can distribute the update through the IoT platform; hospital staff then complete the installation with a single click.

3.3 Data Collection and Analysis

a) Acquisition of Device-Operation Data

In an IoT environment, every connected device generates continuous streams of data — operating conditions, usage frequency, total run time, fault logs, etc. Hospitals can aggregate these data into comprehensive device-operation databases, forming a solid foundation for effective management and timely maintenance. For instance, electrocardiograph monitors can log each use, the number of patients monitored, and specific metric values. Deep analysis of these records enables administrators to assess actual performance and reliability.

b) Data-Driven Decision Support

Advanced analytics applied to operational data yield insights that support evidence-based decision-making in device allocation [6]. By examining usage patterns — frequency and duration — hospitals can reconfigure device placement, situating high-demand units in locations where they are most needed to boost efficiency. Analytics also help predict component lifespans and replacement schedules, guiding budget-planning for procurement. Analysis of fault-record trends can identify common failure modes, enabling targeted corrective actions to improve device quality and stability.

c) Evaluation of Medical Quality

Operational data from medical devices correlate closely with care quality. In the operating room, for example, analysis of anesthesia-machine logs — gas concentration, flow rates, patient vitals — can assess the adequacy of anesthesia delivery and detect safety deviations. If usage data deviate from expected ranges during a given period, it may signal an underlying issue requiring immediate investigation, thus enhancing overall service quality.

3.4 Optimized Equipment Allocation

a) Usage-Efficiency Analysis

IoT systems provide real-time metrics on device demand and utilization. By identifying under-used or over-used units, hospitals can take corrective measures — rescheduling usage or re-allocating resources — to improve overall efficiency [7]. For instance, if an electrocardiograph monitor is under-utilized in one department but over-booked in another, data-driven reallocation can balance the load and maximize utility.

b) Demand Forecasting and Resource Planning

IoT-enabled analytics can forecast future equipment needs based on patient-volume trends and service expansion, supporting better procurement planning. Anticipating demand prevents shortages that could delay care. For example, if a department expects a surge in patient visits, predictive models can signal the need for additional devices, enabling timely acquisition and stockpiling.

c) Cross-Departmental Sharing

In large hospitals, demand imbalances across departments are common. IoT platforms facilitate an equipment-sharing model: when one department's device is idle, another can request temporary use through the system, increasing overall utilization [8]. For instance, an ultrasound unit that finishes morning cases in one department can be scheduled in the afternoon by another, streamlining sharing and optimizing deployment.

4 Challenges in Applying IoT to Medical Device Management

4.1 Data Security and Privacy Protection

Medical device management involves sensitive information — patient identity, usage logs, operational data — and IoT-driven transmission and storage expose these to potential breaches. Unauthorized access to patient records can cause distress and financial loss, while theft of operational data may undermine an institution's competitive position. Hence, robust encryption, access controls, and secure network architectures are critical to safeguard data integrity and confidentiality [9].

4.2 Device Compatibility and Standardization

The market offers a wide array of medical devices from different manufacturers, each with proprietary interfaces and communication protocols. Poor interoperability raises integration costs and complicates system maintenance. For example, connecting a third-party infusion pump and patient monitor may require custom adapters or protocol converters, increasing both financial burden and system complexity. The lack of unified standards hampers large-scale adoption of IoT across heterogeneous device ecosystems.

4.3 Rapid Technological Evolution and System Upgrades

IoT technology evolves rapidly, with new communication protocols and analytical algorithms continually emerging [10]. To remain effective, healthcare institutions must update their IoT platforms accordingly. However, some hospitals lag in technology adoption, leaving them unable to leverage cutting-edge features and compromising management accuracy and efficiency.

4.4 Shortage of Multidisciplinary Talent and Operational Support Challenges

Effective implementation of IoT in medical device management demands professionals who combine clinical knowledge with IT expertise. Such interdisciplinary talent is in short supply. Hospitals often lack structured training programs to cultivate these skills, and competitive recruitment poses difficulties due to limited budgets or career incentives. Talent gaps hinder timely system maintenance and evolution, undermining long-term stability and performance of IoT-based management platforms.

5 Optimization Strategies for IoT-Enabled Medical Device Management

5.1 Strengthening Data Security

a) Establish a Comprehensive Data-Security Framework

Developing a robust data-security framework is the cornerstone of protecting sensitive information [11]. Hospitals should implement strict access-control policies that clearly delineate which roles may view, modify, or delete different categories of data, thereby preventing unauthorized access. For example, only duly authorized personnel should be permitted to retrieve patient medical records or device-operation logs, and every access event must be exhaustively logged and audited. Standardized procedures for data entry, modification, and deletion should be codified to preserve data accuracy and integrity throughout its lifecycle.

b) Deploy Advanced Encryption Methods

To safeguard data in transit and at rest, hospitals must intensify the application of encryption technologies. A hybrid approach — combining symmetric and asymmetric encryption — can be used to encrypt sensitive patient and device data, such that only credentialed users can decrypt and view it. During transmission, secure communication protocols such as HTTPS or SSL/TLS should be enforced, preventing eavesdropping or tampering.

c) Implement Rigorous Backup and Recovery Mechanisms

Regular data backups are essential to mitigate the risk of loss. Backed-up data should be stored in geographically dispersed locations to guard against natural disasters or human error. In addition, a well-defined disaster-recovery plan — complete with periodic restoration drills [12] — ensures that, in the event of data corruption or deletion, critical datasets can be restored swiftly and accurately to maintain uninterrupted clinical operations.

d) Enhance Network-Security Monitoring

Hospitals must invest in network-security infrastructure — firewalls, intrusion-detection systems (IDS), intrusion-prevention systems (IPS), and the like — to continuously monitor traffic for malicious activity. An early-warning system should be established to flag anomalous behavior and trigger prompt incident response. Regular vulnerability scanning and patch management of the IoT platform will further harden defenses and ensure ongoing system resilience.

5.2 Promoting Device Standardization

a) Advance Unified Standards and Protocols

Professional associations and regulatory bodies should collaborate to develop universal interface and communication standards for IoT-enabled medical devices. Standardization enhances interoperability and reduces development and maintenance costs [13]. A comprehensive standard would specify hardware connectors, software APIs, data-format schemas, and communication rules, enabling seamless integration across devices from different manufacturers.

b) Encourage Manufacturer Participation

Device makers should be incentivized — via policy levers or funding programs — to design and produce equipment in compliance with these unified standards. A formal certification scheme can recognize and label devices that meet interoperability criteria, guiding hospitals in procurement decisions.

c) Drive Outreach and Education on Standards

Widespread adoption requires raising awareness among both healthcare providers and manufacturers. Workshops, seminars, and technical symposia should explain standard requirements, share best practices, and showcase successful implementations. An online standards-information portal can centralize updates, technical documentation, and guidance to support smooth adoption.

5.3 Increasing Investment in R&D

a) Foster Hospital–Industry–Academia Collaborations

Hospitals should allocate dedicated funding and resources to IoT research, partnering with universities, research institutes, and technology firms to co-develop innovative solutions [14]. Clinical sites can offer real-world testbeds, academia can supply domain expertise and talent, and industry can provide project management and pathways to commercialization. For instance, a joint project might collect large-scale device-operation datasets and apply machine-learning techniques to build predictive-maintenance models, thereby improving failure-prediction accuracy and reliability.

b) Monitor Emerging Technologies

Staying abreast of front-line developments — 5G communications, edge computing, blockchain, and beyond — enables healthcare organizations to integrate new capabilities as they mature. The ultra-low latency and high bandwidth of 5G, for example, open doors for real-time, high-definition video feeds from surgical suites or remote-control of critical equipment. Blockchain could offer immutable audit trails for device logs, enhancing both data integrity and privacy.

c) Implement Continuous System Upgrades

To remain aligned with evolving clinical and technical requirements, IoT platforms must undergo periodic performance optimizations and feature enhancements. A structured upgrade roadmap — guided by user feedback and industry trends — should dictate when and how new functionalities are deployed. Rigorous testing and validation protocols will ensure that updates do not disrupt ongoing operations.

5.4 Bolstering Talent Development and Recruitment

a) Expand Specialized Academic Programs

Hospitals and educational institutions should co-develop curricula that blend core medical sciences with information-technology disciplines — IoT fundamentals, data analytics, software engineering, and cybersecurity. Joint training initiatives and internship placements will equip graduates with the interdisciplinary skills crucial for managing networked medical devices.

b) Strengthen In-House Training

Current staff must also upskill. Regular workshops and certification courses can familiarize clinical engineers and IT personnel with IoT architectures, system-administration tools, and incident-response protocols. Inviting external experts to share case studies and best practices will broaden institutional know-how and foster a culture of continuous learning.

c) Institute Competitive Recruitment and Retention Policies

To attract and retain top talent, hospitals should offer market-competitive salaries, clear career-advancement pathways, and recognition programs that reward innovation in IoT deployment. Performance-based incentives and research grants can motivate technical staff to pursue cutting-edge projects and ongoing professional growth.

5.5 Optimizing Cost-Benefit Management

a) Strategic Investment Planning

Before deploying IoT solutions, hospitals must conduct needs assessments and cost-benefit analyses tailored to their size, case mix, and strategic goals [15]. Phased rollouts — prioritizing high-impact use cases — can help manage capital expenditures and demonstrate early returns on investment.

b) Control Operating Expenses

Day-to-day costs can be curtailed through intelligent maintenance scheduling (avoiding unnecessary service calls), selection of energy-efficient devices, and streamlined management workflows. Predictive maintenance alone can significantly reduce unplanned downtime and repair costs.

c) Establish a Quantitative Evaluation Framework

A multidimensional assessment system — combining economic, clinical, and social metrics — should be devised to measure the impact of IoT interventions on service quality, patient safety, and organizational efficiency. Both quantitative indicators (cost savings, device-uptime rates) and qualitative outcomes (staff and patient satisfaction) will guide adjustments to strategy and ensure maximal benefit realization.

6 Conclusion

In summary, IoT technology offers transformative potential for medical-device management — enhancing real-time monitoring, streamlining maintenance, and enabling data-driven decision making. Yet, its implementation is accompanied by challenges in data security, interoperability, technological evolution, and human-resource capacity. By adopting the optimization strategies outlined — strengthening cybersecurity, standardizing devices, investing in R&D, cultivating interdisciplinary talent, and rigorously managing costs — healthcare institutions can surmount these obstacles and accelerate the deep integration of IoT into clinical workflows. As intelligent-care demands continue to grow and IoT technologies advance, proactive engagement by hospitals, regulators, and industry partners will be essential to sustain healthy, scalable development in this critical domain.

Acknowledgments

Not applicable.

Conflicts of Interest

The authors declare no conflicts of interest.

Author Contributions

The author contributed solely to the article.

Ethics Approval and Consent to Participate

No ethical approval was required for this review article.

Funding

This research received no external funding.

Availability of Data and Materials

The data presented in this study are available on request from the corresponding author.

Supplementary Materials

Not applicable.

References

[1] Chen HJ. Research on the Application of Internet of Things Technology in Medical Device Management [J]. *Die & Mould Manufacture*, 2024, 24(7):216-218.

[2] Zhou QQ and Lu J. Application Status of Internet of Things Technology Based on UDI in Whole-Life Cycle Information Management of Medical Devices [J]. *China Medical Devices*, 2024, 39(6):161-167.

[3] Bai WH, Wang C and Zhang L. Exploration and Application of Internet of Things Technology in the Management of Removable Medical Devices [J]. *Chinese Hospital Management*, 2023, 43(2):72-74.

[4] Lipsa S , Dash KR and Ivković N. An interpretable dimensional reduction technique with an explainable model for detecting attacks in Internet of Medical Things devices [J]. *Scientific Reports*, 2025, 15(1):8718-8718.

[5] Luo HW. Application of Microwave Technology in Medical Device Testing [J]. *Technology and Information*, 2024(22):169-171.

[6] Zhang XH, Shi J, Yang YH, et al. Application of information-based traceability system in the whole process management of foreign medical devices in disinfection supply center [J]. *China Modern Medicine*, 2024, 31(30):130-134.

[7] Jiang HY. The Application of Medical Device Clinical Trial Information Management Platform in Clinical Trial Management [J]. *Medical Equipment*, 2024, 37(18):39-41+46.

[8] Cheng ZY. Application of Information System in Medical Device Management and Maintenance [J]. *Chinese Community Doctors*, 2024, 40(26):160-162.

[9] Imed DB, Mousameh E, Meriam A B, et al. Edge Devices for Internet of Medical Things: Technologies, Techniques, and Implementation [J]. *Electronics*, 2021, 10(17):2104-2104.

[10] Zheng DP, Zhang YM and Huang YX. Application Analysis of Information Technology in Hospital Medical Device Management [J]. *China Medical Device Information*, 2024, 30(11):161-163.

[11] Wang X. Design and Implementation of the Medical Equipment Maintenance Management System Based on Internet of Things Technology [J]. *Office Informatization*, 2024, 29(5):31-33.

[12] Arefin SM, Rahman M M, Hasan TM, et al. A Topical Review on Enabling Technologies for the Internet of Medical Things: Sensors, Devices, Platforms, and Applications [J]. *Micromachines*, 2024, 15(4):479.

[13] Xia HJ and Ye P. Design of Medical Device Lifecycle Management System Based on Technology of Internet of Things [J]. *Modern Hospital Management*, 2023, 21(6):99-102.

[14] Fu J. Research on Medical Device Management Supported by Internet of Things Technology [J]. *Technology and Health*, 2023, 2(17):125-128.

[15] Bu LP and Dai XB. Exploration of Medical Equipment Management Based on Internet of Things Technology [J]. *China Health Industry,* 2023, 20(16):220-222+227.