Scholar Publishing Group
Machine Learning Theory and Practice
https://doi.org/10.38007/ML.2026.060108
ISSN 2790-0983 Vol. 6, Issue 1: 68-76

# *Analysis of the Current Status of IoT Technology Evolution and Typical Application Scenarios for Smart Healthcare and Industrial Interconnection*

**Dexi Chen**

*School of Computer and Big Data, Jining Normal University, Ulanqab 012000, Inner Mongolia, China*

***Keywords:*** Internet of Things; Smart Healthcare; Industrial Internet; Edge Computing; 5G Convergence; Data Governance

***Abstract:*** The Internet of Things (IoT) is a crucial infrastructure connecting the physical world and digital systems, evolving from one-way sensing and remote monitoring to comprehensive sensing, transmission, computing, decision-making, and services. This paper, focusing on the current state of IoT technology development and typical application scenarios, further narrows its scope to the technological evolution, architectural bottlenecks, and application implementation of smart healthcare and the Industrial Internet. After reviewing English literature and publicly available statistics from the past three years, this paper systematically discusses the latest developments in IoT in terms of connection scale, architecture, edge intelligence, 5G integration, and industry penetration. Key issues are raised from the perspectives of heterogeneous access, real-time limitations, data governance, security and privacy, standard fragmentation, and operational complexity, and an application strategy for various scenarios is proposed. The research indicates that future IoT development should not only focus on increasing the number of connections but also on trusted interconnection, edge-cloud collaboration, scenario closed loops, and value computability to form a high-quality development model.

## 1 Introduction

As sensor technology, embedded system technology, low-power communication technology, cloud platform technology and artificial intelligence algorithms continue to develop, the Internet of Things has become the basic architecture of the digital economy. Compared with the early research that only focused on device online rate and data cloudification, current research focuses more on closed-loop collaboration that connects sensing and data collection and business decision-making in complex scenarios. Recent literature reviews show that the focus of Internet of Things research has shifted from the original architecture discussion to the construction of cross-domain applications, multi-layer collaboration, scalable governance and trusted security systems [1]. Industry-level deployment is no

longer limited to smart homes, but has penetrated into high-value fields such as smart healthcare, smart manufacturing, smart transportation, precision agriculture and public services [2].

However, there are still obvious contradictions in the large-scale deployment of the Internet of Things (IoT). The number of connections is increasing rapidly, and the number of terminals, data volume, and business demand are rising at the same time. Meanwhile, problems such as the coexistence of heterogeneous protocols, platform fragmentation, unstable latency, high energy consumption, and weak security governance are constantly hindering the release of its value [3]. Therefore, it is not enough to measure the development of IoT by the availability of technology alone. It is also necessary to consider factors such as scenario adaptation, governance capabilities, and long-term operation and maintenance efficiency. Therefore, this paper analyzes the current status of technology, problem identification, and strategy optimization from three aspects. Taking smart healthcare and industrial interconnection as entry scenarios, it explores the application path of IoT from quantitative change to qualitative change.

## 2. Current Status Analysis of the Research Topic

The current development status of the Internet of Things is mainly reflected in three aspects. First, the global connection scale continues to grow, and the objects of connection have expanded from consumer terminals to industrial equipment, medical instruments, energy systems, urban infrastructure and other aspects. Second, the system architecture has changed from the original "end-cloud" two-layer architecture to the current "end-edge-cloud-intelligence" three-layer architecture. In this process, edge computing and edge intelligence have become important supports for controlling latency, reducing bandwidth consumption and improving autonomy [4]. Third, in various application scenarios such as smart healthcare, industrial equipment operation and maintenance and smart city public services, the Internet of Things has gradually penetrated into the core business processes [5].

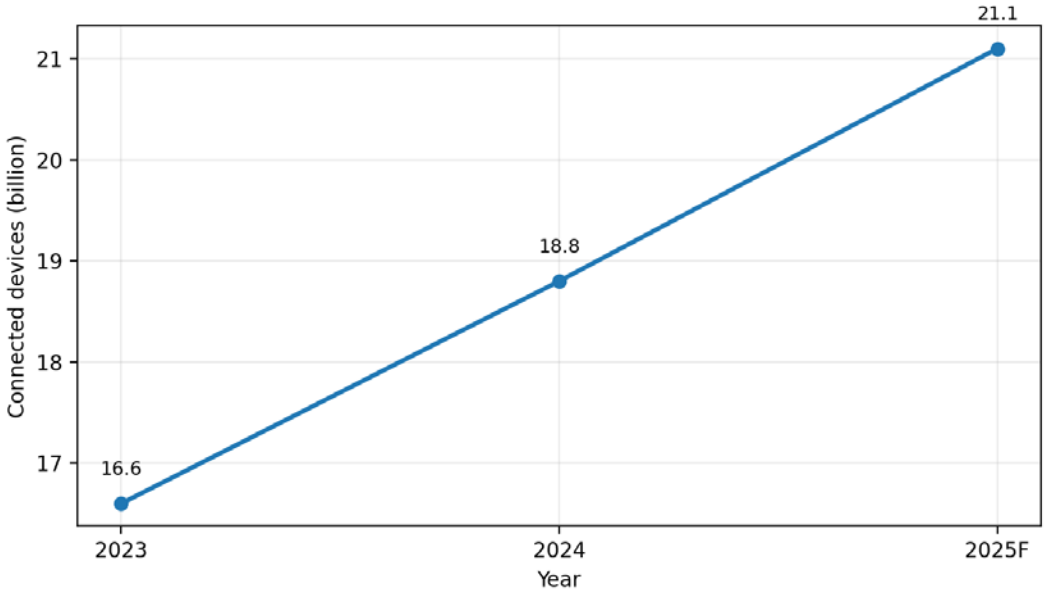


*Figure 1. Global annual growth rate of connected IoT devices (2023-2025, in tens of thousands)*

From a statistical perspective, IoT Analytics data shows that the number of connected IoT devices worldwide increased from 16.6 billion in 2023 to 18.8 billion in 2024, and is expected to reach 21.1 billion in 2025. This indicates that the expansion of connectivity is still ongoing, but the growth pattern has changed from "wide coverage" to "high-value connectivity". Meanwhile, Eurostat's statistics on the use of IoT terminals by EU residents in 2024 show that connected TVs, wearable devices, game consoles and smart speakers account for a large proportion. Consumer IoT has formed a stable base, but service-oriented devices such as home energy, security and health still need further improvement [7]. Both sets of data together illustrate that the competition in the next stage of IoT is not about increasing nodes, but about improving the degree of device collaboration, expanding scenarios to the internal, and realizing a business closed loop.

As the graph shows, the number of global IoT connections has been steadily increasing, with approximately 450 million new terminals added in recent years. This indicates that the IoT is transitioning from pilot testing to large-scale deployment. It's important to note that an increase in the number of connections does not necessarily lead to a corresponding improvement in application quality. If platform architecture, edge processing, and security governance capabilities are insufficient, then scaling up will increase system complexity and expand the attack surface. Therefore, studying the structural changes behind this "growth" is more valuable than simply focusing on the total number of devices.

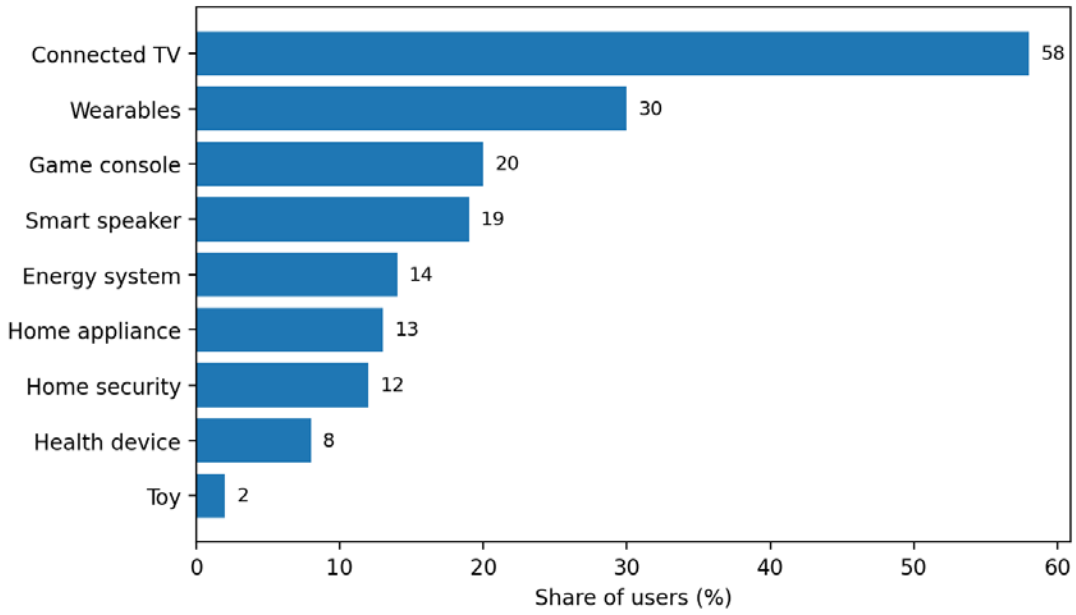


*Figure 1. Shows the changes in the usage rate of different types of IoT devices among EU residents.*

Figure 2 illustrates the structural distribution of consumer-grade IoT devices. Connected TVs and wearables account for a relatively high proportion, indicating that entertainment and personal health are the most readily accepted IoT entry points for users. Home security, health devices, and smart toys account for a lower proportion, suggesting that these scenarios are still constrained by factors such as cost, privacy sensitivity, data reliability, and user habits. Therefore, it can be concluded that when researchers create typical use cases, they should consider the cognitive burden borne by users and the service benefits obtained, and should not only focus on the feasibility of the technology.

*Table 1 Comparison of Evolution Characteristics of Key Technology Layers in the Internet of Things*

| Layer | Core technology | Current maturity | Typical value | Main bottleneck |
|---|---|---|---|---|
| Perception | Sensor, RFID, MCU | High | Low-cost sensing | Power and accuracy |
| Network | NB-IoT, Wi-Fi, 5G, BLE | Medium-High | Wide connectivity | Protocol heterogeneity |
| Edge | Gateway, edge AI, stream processing | Medium | Low latency response | Resource constraint |
| Cloud | Data lake, digital twin, orchestration | High | Global coordination | Bandwidth cost |
| Application | Industry app, hospital app, city service | Medium | Business closed loop | Interoperability |

As shown in Table 1, the perception layer, network layer, edge layer, cloud layer, and application layer do not develop in isolation, but rather evolve together through mutual influence. Currently, the perception layer and cloud layer are relatively mature, but the edge layer and application layer still have significant room for value creation. Insufficient computing power, high energy consumption, and difficulties in adapting to industry standards and business processes, as well as platform integration, will all become bottlenecks in their development. Therefore, IoT research has shifted from breakthroughs in single technologies to the collaborative optimization of the edge, cloud, and device layers—a trend consistently emphasized in recent years' architecture reviews.

From the perspective of literature analysis, the research in the past three years can be roughly divided into four major hot topics. The first category focuses on the overall architecture and methodology of IoT systems, with the integrated development, simulation, deployment, and operation and maintenance of IoT systems being given top priority [1][6]. The second category focuses on industry scenarios, namely medical, industrial, and smart city, mainly analyzing business value and implementation obstacles [5][8]. The third category focuses on security governance and access control, taking identity, authorization, trusted execution, and cross-platform governance as the decisive factors for large-scale applications [9][10]. The fourth category focuses on the integration of 5G, edge computing, and AIoT, attempting to improve the real-time performance and autonomy of the system through network and intelligent capabilities [8]. This has led to the transformation of the Internet of Things from the original "collection of networked technologies" to the current "digital infrastructure system".

To quantitatively measure the efficiency of IoT system deployment, this paper first uses the connection density metric to measure the arrangement of devices in a unit space or business area.

$$C = N / A \tag{1}$$

In equation (1), C is the connection density, N is the number of online devices, and A is the service area. This indicator is suitable for use in places such as parks, workshops, and hospital wards, and can be used to determine whether the coverage of the sensing layer is sufficient. However, excessively high connection density can also cause wireless interference, increased energy consumption, and excessive gateway load, so it needs to be considered in conjunction with capacity planning.

Transmission latency is a crucial parameter affecting the quality of IoT services, impacting both data acquisition and edge uploading. If queuing congestion is ignored, the latency for a single report can be expressed as…

$$T = D / B + L \quad (2)$$

Total latency is the sum of latency values, data volume is the amount of data to be transmitted, link bandwidth is the link bandwidth, and fixed link propagation and processing overhead is represented by L. This formula shows that bandwidth improvement cannot infinitely reduce latency because the fixed processing overhead still exists. This is one of the reasons why edge computing is widely used in IoT architectures, that is, it can reduce latency (D) by leveraging local preprocessing and reduce the frequency of cross-layer transmission.

## 3. Raise questions

Although the application boundaries of the Internet of Things are constantly expanding, there are still many limiting factors in actual engineering and social governance. First, the heterogeneity problem is very serious. There is no unified standard for equipment manufacturers, communication protocols, data models and platform interfaces, resulting in high cross-domain interconnection costs, difficult system migration and poor scalability [3]. Many projects run smoothly in the early pilot stage, but after entering the environment of multi-supplier, multi-scenario and multi-business collaboration, problems such as inconsistent data interfaces, inconsistent semantic tags and broken operation and maintenance links will soon be exposed.

Secondly, the conflict between real-time performance and reliability is widening. Typical scenarios such as smart medical monitoring, industrial predictive maintenance, and urban emergency response have high requirements for millisecond or second-level response times, and cloud-centralized architectures cannot adequately guarantee low latency. When edge node resources are scarce, network jitter occurs, or terminal status is unstable, the time lag between data reporting and decision execution is further amplified, leading to a decrease in the reliability of system operations.

*Table 2 Comparison of Value and Constraints in Typical Application Scenarios*

| Scenario | Main devices | Core data | Primary value | Key constraint |
|---|---|---|---|---|
| Smart hospital | Wearable, monitor, bed sensor | Vital signs | Continuous care | Privacy and reliability |
| Industrial IoT | PLC, camera, vibration sensor | Equipment state | Predictive maintenance | Latency and interoperability |
| Smart city service | Meter, camera, traffic node | Public operation | Resource optimization | Cross-domain governance |
| Smart home | TV, speaker, appliance | User behavior | Convenience | Trust and low stickiness |

Table 2 shows that different scenarios have different requirements for IoT capabilities. Smart healthcare emphasizes privacy protection and continuous service, industrial environments prioritize low latency and high reliability, and smart cities value data collaboration between departments and governance systems. Because scenario requirements differ, if the IoT platform adopts the idea of "one architecture serving all scenarios," it will result in redundant system configurations or the lack of important functions. Therefore, scenario-based layered design should be the starting point for subsequent strategy formulation.

Furthermore, security and privacy have become major constraints on the high-quality development

of the Internet of Things (IoT). Access control, device authentication, firmware update trustworthiness, data minimization, and cross-platform security governance have been increasingly emphasized in recent years' research. Compared to traditional internet systems, the IoT involves a vast number of devices with varying capabilities, many of which are unattended. Insufficient authentication mechanisms or inadequate upgrade processes can amplify system risks instantly. Particularly in smart healthcare environments, the leakage or alteration of sensitive health data can directly impact the security of medical care and societal trust.

Finally, the methodology for development and operation is still immature. Existing research shows that IoT systems generally include hardware access, software writing, communication coordination, data management, and business model planning, and monolithic software development methods are difficult to meet its complexity[6]. The costs of device lifecycle management, policy version control, model updates, and anomaly tracking in the later stages of the project are much higher than those of ordinary information systems, resulting in many projects being "deployable but difficult to run for a long time".

To better reflect the resource consumption during stable system operation, the average energy consumption per unit device can be used for measurement.

$$E\_avg = (E\_1 + E\_2 + \ldots + E\_n) / n \tag{3}$$

Equation (3) is the average energy consumption E_avg = sum of energy consumption / number of nodes. This indicator can be used to evaluate the energy-saving performance of different access methods, sampling rates, and edge processing methods. For terminals powered by batteries, average energy consumption directly affects its maintenance frequency and the continuous online time of the system.

System reliability can also be approximated by a data transmission success rate.

$$R = S / M \tag{4}$$

In equation (4), R represents reliability, S is the number of messages successfully received and available, and M is the total number of messages sent. This indicator is particularly significant in fields such as hospital monitoring, industrial alarms, and urban sensor monitoring, because a high online rate does not necessarily mean a high availability rate. Only when messages arrive stably and are correctly parsed can the system truly generate business value.

## 4. Problem Solving and Optimization Strategies

Regarding the above issues, this paper argues that the improvement of IoT technology should be carried out simultaneously from three aspects: architecture, governance, and scenarios. First, in terms of architecture, a layered structure of end-edge-cloud collaboration should be created. For high-frequency, low-latency, and highly autonomous tasks such as industrial equipment status monitoring and continuous monitoring of vital signs in wards, data can be cleaned, preliminarily inferred, and anomaly judged at the edge, and only the summary, alarms, and model parameters are transmitted to the cloud. This can not only reduce the burden on the link, but also shorten the business response time [8].

Secondly, governance should strengthen standard interfaces, device identity, and access control. Recent access control research shows that traditional RBAC is no longer sufficient to meet the requirements of dynamic, heterogeneous, and cross-domain IoT environments. ABAC, context-aware

authorization, and trusted execution mechanisms should be combined. Unified device identity, hierarchical authorization, the principle of least privilege, and firmware integrity verification can reduce risks during device access and maintenance. Simultaneously, a cross-platform data dictionary and a unified semantic model should be created to reduce later system integration costs.

*Table 3. Strategy Framework for Multi-Scenario Deployment*

| Problem | Technical cause | Optimization strategy | Expected effect |
|---|---|---|---|
| Protocol fragmentation | Vendor-specific stack | Standard API + semantic model | Lower integration cost |
| High latency | Cloud-only workflow | Edge processing + local cache | Faster response |
| Security risk | Weak identity and update chain | Zero-trust access + trusted update | Risk reduction |
| Energy pressure | High sampling and transmission | Adaptive sampling + event trigger | Longer device life |
| Operation complexity | Multi-layer lifecycle mismatch | Unified observability and orchestration | Stable maintenance |

Table 3 shows the correspondence between problem identification and strategy configuration. As the figure shows, the key contradictions in IoT systems are generally not caused by a single technical defect, but rather by the combined effects of devices, networks, platforms, and business processes. Therefore, the solution should not remain at the level of single patch improvements, but should form a sustainable strategy combination. In large-scale industry applications, unified observability, unified orchestration, and unified identity governance are more effective in improving the long-term stability of the system than adding a single new algorithm model.

Third, in terms of scenarios, "high-value closed loop priority" should be implemented. In smart healthcare, ward monitoring, chronic disease follow-up, and in-hospital asset tracking are typical scenarios for predictive maintenance, energy management, and quality inspection of industrial Internet equipment, which can better test the value of technology [5][10]. However, if the application goal is only to connect the equipment to the platform, there is a lack of motivation for continuous operation. Therefore, IoT projects should be driven by business indicators, such as alarm response time reduction rate, equipment downtime reduction rate, and nursing inspection efficiency improvement rate.

Fourth, 5G, AI, and digital twins should be regarded as enhanced capabilities, rather than simply added together. 5G can improve large-scale connectivity and latency, but its benefits depend on appropriate scenario requirements and network planning. AI can improve the efficiency of anomaly detection and resource scheduling, but the premise is that data quality is controllable and the model update mechanism is complete. Digital twins can enhance visualization and prediction capabilities, but without good real-time basic data, its role will be greatly reduced [1][8]. Therefore, the integration of new technologies should be based on systematic adaptation, and the integration of new technologies should not be pursued for the sake of conceptual hot spots.

From a comprehensive effectiveness perspective, the scenario benefit index can be used to measure the effectiveness of IoT construction.

$$V = \alpha R + \beta Q - \gamma C\_o \tag{5}$$

In equation (5), the comprehensive value is represented by V, the reliability benefit by R, the service

quality improvement by Q, and the operating cost by C_o, with weighting coefficients of α, β, and γ, respectively. This equation illustrates that the evaluation of IoT projects cannot only consider technical performance, but also cost control and business benefits. If the increase in reliability and service quality cannot offset the increase in new operation and maintenance costs, then even if the project is the most technologically advanced, it cannot be truly implemented.

Based on the above analysis, this paper proposes the following three implementation suggestions: First, for high real-time scenarios, create an edge-first data flow design to ensure that critical control links are localized as much as possible; second, for highly sensitive scenarios, create a zero-trust access and fine-grained authorization system to make security a basic capability; third, for long-term operation, create a unified monitoring, device profiling, model governance, and asset ledger mechanism to enable the IoT platform to have the engineering characteristics of being "observable, manageable, auditable, and evolvable".

## 5. Conclusion

Therefore, IoT technology has evolved from simply expanding connectivity to expanding value. With increasing global interconnectivity, improved edge-cloud collaboration, and deeper industry applications, it's easy to foresee that the IoT is moving from the proof-of-concept stage to becoming infrastructure. However, issues such as heterogeneous protocols, real-time bottlenecks, security governance, imperfect development methodologies, and long-term operational complexity still exist.

This paper focuses on smart healthcare and industrial internet, analyzing the current state of IoT technology development, main application areas, and key challenges based on English literature and publicly available data from the past three years. The research concludes that the future development of IoT should follow four principles: scenario-driven, edge-first, trusted governance, and value-oriented. After establishing a unified identity, standardized interfaces, edge-cloud collaboration, and full lifecycle operation and maintenance framework, the system will transition from a "connectable" stage to a "sustainable, governable, and value-added" stage. Only in this way can IoT provide a more stable, in-depth, and large-scale supporting foundation for digital China, smart cities, and industrial transformation.

## References


[1] *Ye, J. (2025). Optimization of Neural Motor Control Model Based on EMG Signals. International Journal of Engineering Advances, 2(4), 1-8.*

[2] *Liu, H. (2025). Research on the Evaluation of User Safety Intervention Measures Based on Causal Inference. Engineering Advances, 5(4).*

[3] *Wang, B. (2025). Strategies and Practices for Load Test Optimization in Distributed Systems. SCIENTIFIC JOURNAL OF TECHNOLOGY Учредители: Boya Century Publishing, 7(2), 132-137.*

[4] *Wang, B. (2025). Research on Load Balancing Technology in Distributed System Architecture. International Journal of Multimedia Computing (2025), 6(1), 152-159.*

[5] *Xiao Ma. Engineering Study of Disaster Recovery and Fault Self-Healing Mechanisms for Distributed Systems under Cross-Regional Deployment Conditions. International Journal of Engineering Technology and Construction (2026), Vol. 7, Issue 1: 1-7.*

[6] *Zhang, Z. (2026). Research on the Design of Scalable Enterprise-Level AI Systems Data Platform Architectures from an SDE Perspective.*

*[7] Zheng, H. (2026). Research on Edge Computing Deep Neural Network Task Unloading Based on Resource Collaboration Framework and Multi Strategy Optimization.*

*[8] Huang, J. (2025, August). Research on Multi-Model Fusion Machine Learning Demand Intelligent Forecasting System in Cloud Computing Environment. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-7). IEEE.*

*[9] Sun, Q. (2026). Research on a Robotic Natural Language Intelligent Decision-Making Framework Based on Large Language Models, Thinking Chain Reasoning, and Multi-Agent Collaboration.*

*[10] Wang, Y. (2026). Research on the Application of Artificial Intelligence in Supply Chain Risk Early Warning.*

*[11] Liu, H. (2026). Research on Dynamic Price Prediction of E-commerce Based on Time Series Modeling.*

*[12] Yu, X. (2026). Strategy Models and Practical Research of Growth Marketing under the Background of Digital Transformation.*

*[13] Hou, Y. (2026). Research on BIOS and BMC Compatibility Optimization Methods for Cross-Generation Servers in Production Environments.*

*[14] Hou, Y. (2026). Research on Server Performance Stability Assurance Mechanisms during Cross-Generation Computing Platform Upgrades.*

*[15] Han, X. (2026). Research on Process Decision-Making Behavior under Incomplete Information Conditions in Automobile Manufacturing Systems.*

*[16] Zheng, H. (2026). Research on Edge Computing Deep Neural Network Task Unloading Based on Resource Collaboration Framework and Multi Strategy Optimization.*

*[17] Zhang, Z. (2026). Research on the Design of Scalable Enterprise-Level AI Systems Data Platform Architectures from an SDE Perspective.*

*[18] Xiao Ma. Engineering Study of Disaster Recovery and Fault Self-Healing Mechanisms for Distributed Systems under Cross-Regional Deployment Conditions. International Journal of Engineering Technology and Construction (2026), Vol. 7, Issue 1: 1-7.*

*[19] Ma, X. (2026). Research on End-To-End Reliability Modeling and Optimization of Service Grid.*

*[20] Zhixian Zhang. Research on Model Engineering Integration Methods for AI Systems Based on Data-Driven Intelligence. International Journal of Big Data Intelligent Technology (2026), Vol. 7, Issue 1: 140-149.*

*[21] Zheng, H. (2026). Research on Edge Computing Network Task Scheduling and Resource Management Optimization Based on Artificial Intelligence Technology.*

*[22] Han, X. (2026). Research on Automotive Manufacturing Process Optimization Methods for Multi-Supplier Collaboration.*

*[23] Yin, J. (2026). Research on Financial Time Series Prediction and Multiscale Correlation Based on the Fusion of Network Big Data and Deep Learning.*

*[24] Yu, X. (2025). Digital Transformation Empowers Growth Marketing with Marketing Data Analysis Integration and Real-Time Display Strategy.*

*[25] Liu, H. (2026). Research on the Application of Causal Reasoning Method in Content Compliance Experimental Evaluation.*

*[26] Sun, Q. (2026). Research on Lightweight Intelligent Dialogue Systems Based on Semantic Entity Enhanced Intention Recognition and Rule Retrieval Generation Hybrid Models.*

*[27] Wang, B. (2025). Research on Load Balancing Technology in Distributed System Architecture. International Journal of Multimedia Computing (2025), 6(1), 152-159.*