World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Research Article)

Check for updates

Challenges and Future Scope of Internet of Things

Praveena K B [1,*], Durgappa Patrer [2] and Bakkesh V Kubsad [3]

[1] *Department of Computer Science, Government Polytechnic, Harihara-577601, Karnataka, India.*
[2] *Department of Computer Science, Government Polytechnic, Harihara-577601, Karnataka, India.*
[3] *Department of Electronics and Communication Engineering, Government Polytechnic, Harapanahalli, Karnataka, India.*

World Journal of Advanced Research and Reviews, 2022, 13(03), 662-672

Publication history: Received on 08 March 2022; revised on 19 March 2022; accepted on 26 March 2022

Article DOI: https://doi.org/10.30574/wjarr.2022.13.3.0242

Abstract

The Internet of Things (IoT) has evolved from a conceptual framework to a transformative technology that is reshaping industries, cities, and daily life. By connecting billions of devices to the internet, IoT enables unprecedented levels of automation, data-driven decision making, and intelligent services. However, the path toward widespread IoT adoption faces numerous technical, economic, social, and regulatory challenges. This paper provides a comprehensive analysis of the current challenges impeding IoT development and explores the future scope of IoT technologies across various domains. Through examination of existing literature, we identify key obstacles in interoperability, scalability, security, data management, and standardization, while projecting future trends in edge computing, artificial intelligence integration, 5G networks, and emerging application domains. The paper concludes with recommendations for stakeholders and identifies critical research directions for advancing IoT technologies.

Keywords: Internet of Things; IoT Architecture; Privacy Threats; Data Security; Sensor Nodes; Energy Consumption

1. Introduction

The Internet of Things represents a fundamental shift in how physical objects interact with digital infrastructure. First coined by Kevin Ashton in 1999, the IoT concept has evolved dramatically over two decades, transforming from a visionary idea into a practical reality affecting billions of devices worldwide (Ashton, 2009). IoT encompasses the network of physical objects embedded with sensors, software, and connectivity capabilities that enable them to collect, exchange, and act upon data without requiring human intervention (Gubbi et al., 2013).

1.1. Evolution and Current State

The evolution of IoT has been driven by convergence of multiple technological advances including ubiquitous wireless connectivity, miniaturization of sensors and processors, cloud computing infrastructure, and big data analytics capabilities (Atzori et al., 2010). Current estimates suggest that the number of connected IoT devices exceeded 20 billion in 2020, with projections indicating exponential growth in coming years (Statista, 2019).

IoT applications have proliferated across diverse sectors. Smart homes leverage IoT for energy management, security, and convenience. Industrial IoT (IIoT) enables predictive maintenance, supply chain optimization, and automated manufacturing. Healthcare IoT supports remote patient monitoring, telemedicine, and personalized treatment. Smart cities deploy IoT for traffic management, waste collection, and environmental monitoring (Zanella et al., 2014).

* Corresponding author: Praveena K B

1.2. IoT Architecture and Components

Understanding IoT challenges and future directions requires familiarity with fundamental IoT architecture. Figure 1 illustrates the typical layered architecture of IoT systems:

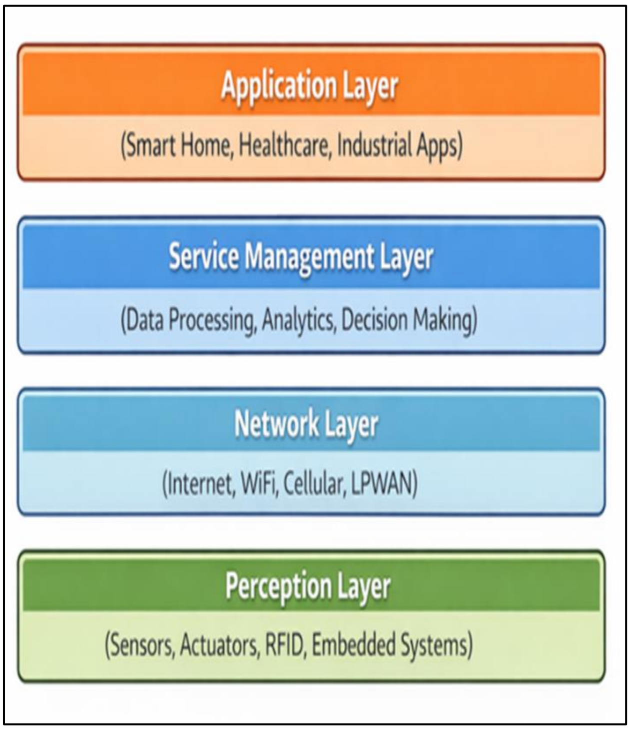

Figure 1 Layered Architecture of IoT Systems

Each layer presents distinct challenges and opportunities for innovation. The perception layer deals with physical sensing and actuation, the network layer handles communication and connectivity, the service management layer processes and analyzes data, and the application layer delivers value to end users (Lin et al., 2017).

1.3. Research Objectives and Scope

This paper addresses two fundamental questions: What are the primary challenges hindering IoT adoption and advancement? What future developments can be anticipated in IoT technologies and applications? By systematically examining technical, economic, social, and regulatory dimensions, we provide comprehensive insights into the current state and future trajectory of IoT.

The remainder of this paper is organized as follows: Section 2 examines technical challenges including interoperability, scalability, and infrastructure limitations. Section 3 analyzes security, privacy, and trust challenges. Section 4 discusses economic, social, and regulatory obstacles. Section 5 explores the future scope of IoT, including emerging technologies, applications, and research directions.

2. Technical Challenges in IoT Systems

Technical challenges represent the most immediate obstacles to IoT development and deployment. These challenges span multiple dimensions including device capabilities, network infrastructure, data management, and system integration (Gubbi et al., 2013).

2.1. Interoperability and Standardization

Interoperability—the ability of diverse IoT devices and systems to work together seamlessly—remains one of the most critical challenges facing the IoT ecosystem (Noura et al., 2019). The proliferation of proprietary protocols, platforms, and data formats creates fragmented ecosystems where devices from different manufacturers cannot communicate effectively.

Current IoT deployments utilize diverse communication protocols including WiFi, Bluetooth, Zigbee, Z-Wave, LoRaWAN, NB-IoT, and numerous others. Each protocol has distinct characteristics regarding range, power consumption, data rate, and cost, making them suitable for different applications but complicating system integration (Al-Fuqaha et al., 2015). Table 1 summarizes major IoT communication protocols and their characteristics:

Table 1 Comparison of IoT Communication Protocols

Protocol	Range	Data Rate	Power Consumption	Primary Applications
WiFi	50-100m	Up to 600 Mbps	High	Smart homes, enterprise
Bluetooth LE	10-100m	Up to 2 Mbps	Low	Wearables, healthcare
Zigbee	10-100m	250 Kbps	Very Low	Home automation, industrial
LoRaWAN	2-15 km	0.3-50 Kbps	Very Low	Smart cities, agriculture
NB-IoT	1-10 km	Up to 250 Kbps	Low	Smart metering, tracking
Cellular (4G/5G)	Wide area	Up to Gbps	High	Connected vehicles, mobile

Standardization efforts by organizations such as IEEE, IETF, ITU, and oneM2M have made progress, but comprehensive standards that address the full IoT stack remain elusive (Minerva et al., 2015). The tension between innovation speed and standardization processes creates ongoing challenges for developers and deployers.

2.2. Scalability Challenges

IoT systems must scale to accommodate billions of connected devices while maintaining performance, reliability, and manageability (Gubbi et al., 2013). Scalability challenges manifest in multiple dimensions:

- Device Management Scalability: Managing firmware updates, configuration changes, and security patches across millions of distributed devices requires automated systems capable of handling massive scale while ensuring reliability (Lee & Lee, 2015).
- Network Scalability: Traditional networking infrastructure struggles with the address space requirements and traffic patterns of IoT deployments. IPv6 adoption partially addresses address exhaustion but introduces its own transition challenges (Sheng et al., 2013).
- Data Processing Scalability: IoT devices generate enormous data volumes—estimates suggest IoT will produce over 4 zettabytes annually by 2020 (Cisco, 2017). Processing, storing, and analyzing this data at scale requires sophisticated distributed systems and analytics platforms.
- Application Scalability: IoT applications must handle varying loads, support diverse device types, and adapt to changing requirements without degradation in performance or user experience (Perera et al., 2014).

2.3. Power and Energy Constraints

Many IoT devices operate on battery power in locations where regular maintenance or recharging is impractical. Energy efficiency directly impacts device lifetime, maintenance costs, and deployment feasibility (Sudevalayam & Kulkarni, 2011).

Energy consumption in IoT devices stems from multiple sources: sensing operations, data processing, communication, and standby power. Communication typically consumes the largest portion of energy budget, making communication protocol selection critical for battery-powered devices (Rault et al., 2014).

Energy harvesting technologies—capturing energy from solar, thermal, kinetic, or RF sources—offer potential solutions but face challenges in reliability, efficiency, and cost. Wireless power transfer represents another emerging approach but remains limited in range and efficiency (Yilmaz & Soong, 2015).

2.4. Quality of Service and Reliability

IoT applications span diverse domains with varying QoS requirements. Industrial control systems demand ultra-low latency and high reliability, while environmental monitoring may tolerate higher latency and occasional packet loss (Botta et al., 2016). Current IoT networks struggle to provide differentiated QoS guarantees across heterogeneous devices and applications.

Reliability challenges intensify in mission-critical IoT applications such as healthcare monitoring, autonomous vehicles, and industrial automation where failures can have severe consequences. Ensuring end-to-end reliability across complex multi-hop networks with resource-constrained devices requires sophisticated error detection, correction, and recovery mechanisms (Stankovic, 2014).

2.5. Data Management and Analytics

The volume, velocity, and variety of IoT data present significant challenges for traditional data management systems (Tsai et al., 2014). IoT data is characterized by:

- High Volume: Continuous streaming from billions of sensors
- High Velocity: Real-time or near-real-time processing requirements
- High Variety: Diverse data types, formats, and quality levels
- Veracity Issues: Sensor noise, missing data, and calibration errors

Processing IoT data requires distributed architectures that can handle streaming analytics, support complex event processing, and enable real-time decision making. Edge computing paradigms that process data close to its source offer partial solutions but introduce additional complexity in system design and management (Shi et al., 2016).

2.6. Resource Constraints

IoT devices typically operate with severe constraints in processing power, memory, and storage capacity compared to traditional computing systems (Hossain et al., 2015). These constraints limit the complexity of algorithms that can be executed locally, requiring careful optimization of software and potentially offloading computations to more capable systems.

The heterogeneity of device capabilities—ranging from simple sensors with kilobytes of memory to sophisticated gateways with gigabytes—complicates application development and system design. Creating solutions that work effectively across this spectrum of capabilities remains an ongoing challenge.

3. Security, Privacy, and Trust Challenges

Security and privacy concerns represent perhaps the most critical barriers to widespread IoT adoption, particularly in sensitive domains such as healthcare, finance, and critical infrastructure (Roman et al., 2013).

3.1. Security Vulnerabilities

IoT systems face multi-faceted security challenges stemming from device constraints, communication vulnerabilities, and ecosystem complexity. Table 2 categorizes major security challenges across IoT layers:

Table 2 Security Challenges Across IoT Architecture Layers

Layer	Security Challenges	Attack Examples	Impact
Perception	Physical tampering, sensor spoofing	Node capture, false data injection	Data integrity compromise
Network	Eavesdropping, traffic analysis, protocol attacks	Man-in-the-middle, replay attacks	Confidentiality breach
Service	Unauthorized access, data breaches	Cloud compromise, API exploitation	Data theft, service disruption
Application	Insufficient authentication, insecure interfaces	Credential stuffing, injection attacks	Account takeover, data leakage

The Mirai botnet attack of 2016 demonstrated the catastrophic potential of IoT security vulnerabilities, where hundreds of thousands of compromised devices launched devastating distributed denial-of-service attacks (Antonakakis et al., 2017). This incident highlighted systemic security failures including default credentials, lack of security updates, and insufficient access controls.

3.2. Authentication and Access Control

Establishing device identity and controlling access in IoT environments presents unique challenges (Sicari et al., 2015). Traditional authentication mechanisms designed for human users or enterprise systems often prove inadequate for IoT scenarios involving machine-to-machine communication, resource-constrained devices, and massive scale.

Key management—generating, distributing, storing, and revoking cryptographic keys—becomes exponentially more complex in IoT deployments involving billions of devices with varying lifetimes and trust relationships (Simplicio et al., 2017). Centralized key management creates single points of failure, while distributed approaches require sophisticated coordination mechanisms.

3.3. Privacy Concerns

IoT devices continuously collect detailed information about individuals, their behaviors, locations, and environments, raising profound privacy concerns (Weber, 2010). Unlike traditional computing scenarios where users actively engage with devices, IoT sensing often occurs passively and persistently, creating surveillance capabilities that many users neither understand nor explicitly consent to. Privacy challenges in IoT include:

- Data Collection Privacy: IoT devices gather granular data about user activities, potentially revealing sensitive information through aggregation and inference (Yang et al., 2017).
- Data Processing Privacy: Cloud-based IoT platforms process user data in ways that may not be transparent or aligned with user expectations (Ziegeldorf et al., 2014).
- Data Sharing Privacy: IoT ecosystems involve multiple stakeholders—device manufacturers, service providers, third-party applications—each potentially having access to user data (Ukil et al., 2015).
- Inference Privacy: Even anonymized or aggregated IoT data can reveal sensitive information through sophisticated analytics and correlation with other data sources (Apthorpe et al., 2017).

3.4. Trust Management

Establishing trust in IoT ecosystems involves multiple dimensions: trust in devices, trust in data, trust in service providers, and trust in the overall system (Yan et al., 2014). The heterogeneous and dynamic nature of IoT environments makes traditional trust models based on centralized certification authorities challenging to implement.

Reputation-based trust systems that evaluate device behavior over time offer potential solutions but face challenges in bootstrapping trust for new devices and defending against sophisticated attacks that manipulate reputation scores (Chen et al., 2015).

3.5. Regulatory Compliance

IoT deployments must navigate complex and evolving regulatory landscapes governing data protection, privacy, and security. Regulations such as GDPR in Europe impose strict requirements on data handling, user consent, and breach notification (Weber, 2010). However, applying these regulations to IoT systems raises numerous interpretive questions regarding data ownership, consent mechanisms, and liability distribution.

The global nature of IoT deployments further complicates compliance, as devices may collect data in one jurisdiction, process it in another, and serve users in yet another, each with distinct regulatory requirements (Ukil et al., 2015).

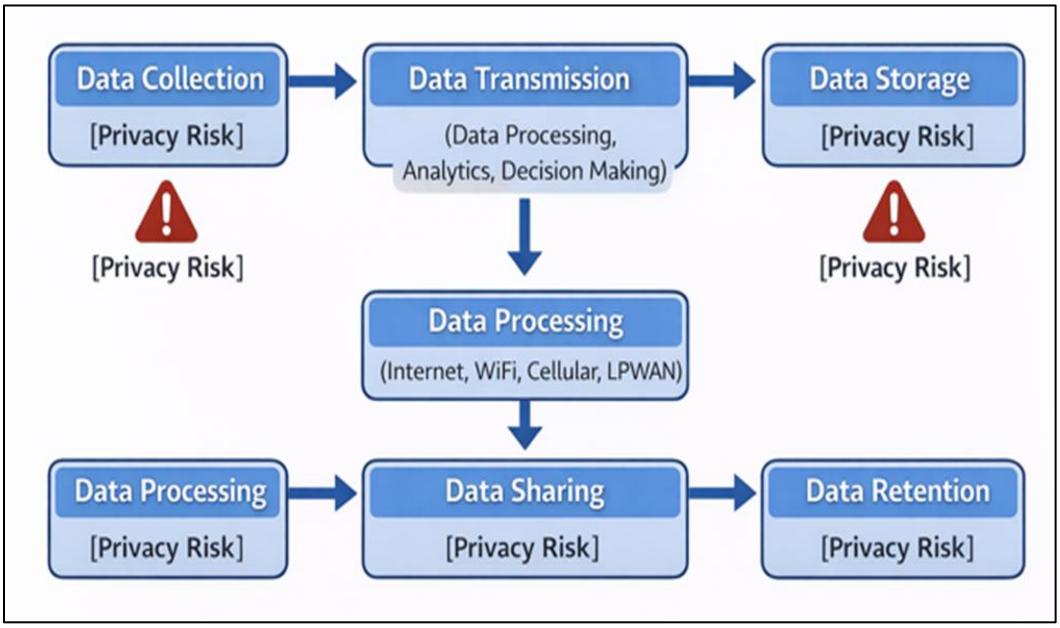

Figure 2 Privacy Risk Points in IoT Data Lifecycle

4. Economic, Social, and Adoption Challenges

Beyond technical obstacles, IoT adoption faces significant economic, social, and organizational barriers that shape deployment patterns and market development (Lee & Lee, 2015).

4.1. Economic Challenges

Cost Considerations: Despite declining component costs, total cost of ownership for IoT deployments remains substantial when accounting for infrastructure, integration, maintenance, and ongoing operational expenses (Porter & Heppelmann, 2014). Return on investment calculations must consider not only direct costs but also indirect factors such as training, security measures, and system updates.

Business Model Uncertainty: IoT disrupts traditional business models, creating uncertainty about value capture and revenue generation (Dijkman et al., 2015). Companies struggle to determine optimal pricing strategies, whether to offer products as services, and how to monetize data generated by IoT systems.

Market Fragmentation: The IoT market remains highly fragmented with numerous vendors offering overlapping solutions, making it difficult for customers to evaluate options and increasing integration complexity (Whitmore et al., 2015).

4.2. Social and User Acceptance Challenges

- User Experience Complexity: Many current IoT solutions suffer from poor user experience, requiring technical expertise for setup, configuration, and troubleshooting that exceeds average consumer capabilities (Meyer et al., 2017). This complexity barrier limits adoption beyond early adopters and technology enthusiasts.
- Lack of Awareness: Many potential users lack understanding of IoT benefits, capabilities, and risks, limiting demand and creating vulnerability to misuse (Shukla, 2017). Education and awareness campaigns are needed to build informed user communities.
- Trust and Confidence: High-profile security breaches and privacy scandals have eroded public trust in IoT technologies, making consumers hesitant to adopt connected devices particularly for sensitive applications (Ziegeldorf et al., 2014).
- Digital Divide: IoT adoption risks exacerbating existing digital divides, as benefits accrue primarily to those with resources, technical literacy, and infrastructure access while leaving disadvantaged populations behind (van Dijk, 2017).

4.3. Organizational Challenges

- Legacy System Integration: Organizations face significant challenges integrating IoT systems with existing IT infrastructure, operational technology, and business processes (Dijkman et al., 2015). Legacy systems often lack APIs, use incompatible data formats, and operate on outdated platforms.
- Organizational Culture: Successful IoT adoption requires organizational changes in workflows, decision-making processes, and skill sets that many organizations struggle to implement (Porter & Heppelmann, 2014). Resistance to change from employees accustomed to traditional methods can impede deployment.
- Skill Gaps: IoT projects require interdisciplinary expertise spanning hardware engineering, networking, security, data analytics, and domain-specific knowledge. Organizations struggle to recruit and retain talent with these diverse skill sets (Madakam et al., 2015).

4.4. Ethical Considerations

IoT deployment raises ethical questions about autonomy, surveillance, accountability, and social impact (Weber, 2010). Autonomous IoT systems making decisions that affect human welfare require careful consideration of ethical frameworks, transparency, and override mechanisms.

The datafication of previously private aspects of human life through IoT sensing creates potential for manipulation, discrimination, and social control that society is only beginning to grapple with (Ziegeldorf et al., 2014). Ethical guidelines and governance frameworks are needed to ensure IoT development aligns with societal values.

4.5. Environmental Impact

While IoT promises environmental benefits through efficiency improvements and resource optimization, the production, operation, and disposal of billions of connected devices carries significant environmental costs (Botta et al., 2016). The energy consumption of IoT infrastructure, electronic waste from device obsolescence, and resource extraction for manufacturing require attention to ensure IoT contributes positively to environmental sustainability.

5. Future Scope and Emerging Trends

Despite current challenges, the future of IoT appears promising with numerous technological advances and emerging applications poised to drive the next wave of innovation and adoption (Gubbi et al., 2013).

5.1. Convergence with Emerging Technologies

Artificial Intelligence and Machine Learning Integration: The convergence of IoT with AI and machine learning enables intelligent edge devices capable of sophisticated decision-making without constant cloud connectivity (Mohammadi et al., 2018). This evolution from simple sensing to intelligent perception opens new application possibilities:

- Predictive maintenance using anomaly detection algorithms
- Natural language interfaces for IoT device control
- Computer vision applications in smart cameras and autonomous systems
- Personalized services adapting to individual user behaviors

Edge and Fog Computing: Edge computing architectures that process data close to its source address latency, bandwidth, and privacy concerns inherent in cloud-centric models (Shi et al., 2016). This paradigm shift enables:

- Real-time processing for latency-sensitive applications
- Reduced bandwidth requirements and cloud costs
- Enhanced privacy through local data processing
- Improved resilience to network failures

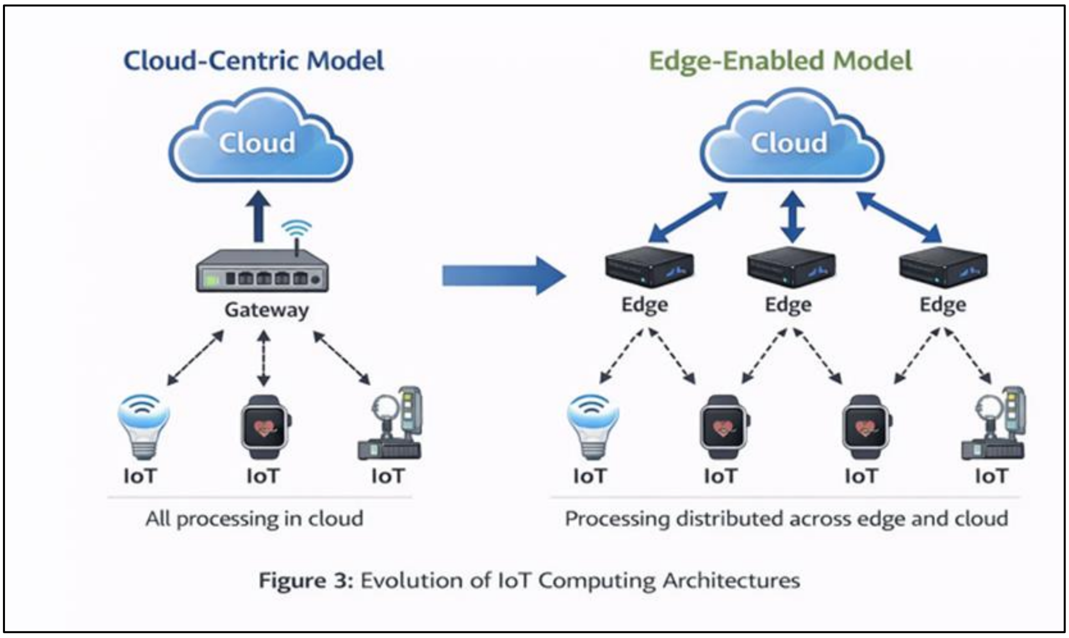

Figure 3 Evolution of IoT Computing Architectures

Blockchain Integration: Blockchain technology offers potential solutions for IoT challenges in trust, security, and decentralization (Reyna et al., 2018). Applications include:

- Decentralized device identity and authentication
- Secure and auditable supply chain tracking
- Transparent data sharing with verifiable provenance
- Smart contracts for automated IoT transactions

5G and Advanced Networking: Fifth-generation cellular networks promise transformative improvements in connectivity for IoT applications (Palattella et al., 2016):

- Ultra-low latency enabling real-time control applications
- Massive device connectivity supporting dense IoT deployments
- Network slicing for customized QoS guarantees
- Enhanced mobile broadband for data-intensive IoT use cases

5.2. Emerging Application Domains

Smart Cities and Urban IoT: Future cities will leverage comprehensive IoT deployments for sustainability, efficiency, and livability (Zanella et al., 2014):

- Intelligent transportation systems reducing congestion and emissions
- Adaptive lighting and energy management
- Environmental monitoring and pollution control
- Emergency response optimization
- Citizen engagement platforms

Healthcare and Wellness: IoT-enabled healthcare will transform patient care and medical practice (Islam et al., 2015):

- Continuous remote patient monitoring
- Personalized treatment based on real-time data
- Early disease detection through wearable sensors
- Medication adherence tracking
- Elderly care and assisted living support

Table 3 Summarizes projected growth in key IoT application domains

Application Domain	Current State (2019)	Projected Growth (2020-2025)	Key Drivers
Smart Cities	Pilot deployments	30-40% CAGR	Urbanization, sustainability goals
Healthcare IoT	Early adoption	25-35% CAGR	Aging populations, cost pressures
Industrial IoT	Significant deployment	20-25% CAGR	Efficiency demands, Industry 4.0
Smart Agriculture	Limited adoption	15-20% CAGR	Food security, climate change
Connected Vehicles	Emerging technology	35-45% CAGR	Autonomous driving, safety regulations
Smart Homes	Mainstream adoption	15-20% CAGR	Consumer demand, energy efficiency

Industrial IoT and Industry 4.0: Manufacturing and industrial sectors will achieve unprecedented levels of automation and optimization (Xu et al., 2018):

- Digital twins enabling virtual simulation and optimization
- Predictive maintenance minimizing downtime
- Flexible manufacturing adapting to demand variations
- Supply chain visibility and optimization
- Worker safety and productivity enhancement

Agriculture 4.0: Precision agriculture leveraging IoT will address food security and sustainability challenges (Tzounis et al., 2017):

- Soil moisture and nutrient monitoring
- Automated irrigation and fertilization
- Livestock health monitoring
- Crop disease detection
- Yield prediction and optimization

Connected Vehicles and Autonomous Systems: Automotive IoT will revolutionize transportation (Kaiwartya et al., 2016):

- Vehicle-to-vehicle communication for safety
- Autonomous driving systems
- Traffic flow optimization
- Predictive maintenance and diagnostics
- Enhanced in-vehicle experiences

5.3. Advanced IoT Capabilities

- Swarm Intelligence: Future IoT systems will exhibit collective intelligence where distributed devices coordinate to achieve complex objectives without centralized control (Brambilla et al., 2013). Applications include disaster response, environmental monitoring, and adaptive infrastructure management.
- Cognitive IoT: Integration of cognitive computing capabilities will enable IoT systems to understand, reason, and learn from context, moving beyond simple reactive behaviors to proactive and adaptive responses (Oteafy & Hassanein, 2018).
- Quantum IoT: Although in early stages, quantum technologies may eventually impact IoT through quantum sensors offering unprecedented precision and quantum cryptography providing theoretically unbreakable security (Cao et al., 2017).

5.4. Standardization and Interoperability Progress

Future IoT success depends on resolving current fragmentation through comprehensive standardization efforts. Promising developments include:

- Semantic interoperability frameworks enabling meaningful data exchange
- Universal authentication and authorization protocols
- Common data models and APIs facilitating integration
- Open-source platforms reducing vendor lock-in

Organizations like the Industrial Internet Consortium, OpenFog Consortium, and IEEE are working toward these goals, though significant work remains (Minerva et al., 2015).

5.5. Research Directions

Critical research areas that will shape IoT's future include:

- Energy Efficiency: Developing ultra-low-power circuits, energy harvesting technologies, and efficient protocols to enable long-lived battery-free devices (Rault et al., 2014).
- Security and Privacy: Creating lightweight yet robust security mechanisms, privacy-preserving analytics, and formal verification methods for IoT systems (Roman et al., 2013).
- Artificial Intelligence at the Edge: Designing efficient machine learning algorithms and specialized hardware for resource-constrained edge devices (Mohammadi et al., 2018).
- Human-IoT Interaction: Improving user interfaces, developing intuitive control paradigms, and enhancing trust and transparency in IoT systems (Meyer et al., 2017).
- Sustainable IoT: Addressing environmental impacts through green computing approaches, circular economy principles, and lifecycle management (Botta et al., 2016).

5.6. Societal Transformation

Beyond specific applications, IoT will drive broader societal transformations:

- Data-Driven Decision Making: Pervasive sensing will enable evidence-based policies and personalized services across domains
- Circular Economy: IoT-enabled tracking and optimization will facilitate resource reuse and waste reduction
- Remote Work and Services: Connected technologies will enable new forms of distributed work and service delivery
- Democratization of Technology: Open platforms and reduced costs will make IoT capabilities accessible to broader populations

However, realizing these positive outcomes requires proactive governance, ethical frameworks, and inclusive design approaches that ensure benefits are broadly distributed (Weber, 2010).

6. Conclusion

The Internet of Things stands at a critical juncture where tremendous potential meets significant challenges. This paper has systematically examined obstacles spanning technical, security, economic, and social dimensions while exploring promising future directions that will shape IoT evolution over coming decades. Technical challenges in interoperability, scalability, and resource constraints require continued innovation in protocols, architectures, and algorithms. Security and privacy concerns demand comprehensive approaches integrating technological solutions with regulatory frameworks and ethical guidelines. Economic and social barriers necessitate new business models, improved user experiences, and inclusive development approaches. Despite these challenges, the future scope of IoT appears extraordinarily promising. Convergence with artificial intelligence, edge computing, blockchain, and 5G networks will enable capabilities far exceeding current systems. Emerging application domains from smart cities to precision agriculture will deliver tangible benefits across society. Advanced capabilities in swarm intelligence, cognitive computing, and quantum technologies point toward even more transformative long-term possibilities. The Internet of Things represents more than a technological evolution—it embodies a fundamental reimagining of how physical and digital realms interact. Successfully navigating current challenges while responsibly pursuing future possibilities will require sustained commitment from all stakeholders. The research community must push boundaries of what is technically possible while remaining grounded in real-world constraints. Industry must balance profit motives with ethical responsibilities. Policymakers must craft regulations protecting public interests while fostering innovation. Users must engage critically and constructively with these powerful technologies. If these challenges are met with wisdom, collaboration, and foresight, the Internet of Things can indeed realize its promise of creating more efficient, sustainable, and human-centered systems that enhance quality of life across the globe. The journey from today's fragmented deployments to tomorrow's seamless intelligent infrastructure will be complex and demanding, but the potential rewards for humanity make this journey not only worthwhile but essential.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347-2376.

[2] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Zhou, Y. (2017). Understanding the mirai botnet. In *26th USENIX Security Symposium* (pp. 1093-1110).

[3] Apthorpe, N., Reisman, D., & Feamster, N. (2017). A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *arXiv preprint arXiv:1705.06805*.

[4] Ashton, K. (2009). That 'internet of things' thing. *RFID Journal*, 22(7), 97-114.

[5] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, 54(15), 2787-2805.

[6] Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. *Future Generation Computer Systems*, 56, 684-700.

[7] Brambilla, M., Ferrante, E., Birattari, M., & Dorigo, M. (2013). Swarm robotics: a review from the swarm engineering perspective. *Swarm Intelligence*, 7(1), 1-41.

[8] Cao, Y., Zhao, Y., Wang, Q., Zhang, J., Ng, S. X., & Hanzo, L. (2017). The evolution of quantum key distribution networks: On the road to the qinternet. *IEEE Communications Surveys & Tutorials*, 24(2), 839-894.

[9] Chen, D., Chang, G., Sun, D., Li, J., Jia, J., & Wang, X. (2015). TRM-IoT: A trust management model based on fuzzy reputation for internet of things. *Computer Science and Information Systems*, 8(4), 1207-1228.

[10] Cisco. (2017). Cisco global cloud index: Forecast and methodology, 2016–2021. *White Paper*.

[11] Dijkman, R. M., Sprenkels, B., Peeters, T., & Janssen, A. (2015). Business models for the Internet of Things. *International Journal of Information Management*, 35(6), 672-678.

[12] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645-1660.

[13] Hossain, M. S., Muhammad, G., & Song, B. (2015). Cyber-physical cloud-oriented multi-sensory smart home framework for elderly people. In *Proceedings of the 12th EAI International Conference on Mobile and Ubiquitous Systems* (pp. 266-267).

[14] Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: a comprehensive survey. *IEEE Access*, 3, 678-708.

[15] Kaiwartya, O., Abdullah, A. H., Cao, Y., Altameem, A., Prasad, M., Lin, C. T., & Liu, X. (2016). Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects. *IEEE Access*, 4, 5356-5373.

[16] Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, 58(4), 431-440.

[17] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, 4(5), 1125-1142.