

## A REVIEW OF THE “INTERNET of THINGS”: FROM ORIGINS TO FUTURE HORIZONS

**Lupulescu (Machidon) Alina-Elena,**

“Constantin Brâncuși” University, Târgu Jiu, ROMANIA

University of Petroșani, Petroșani, ROMANIA

**ABSTRACT:** This article outlines the development of the IoT. Over the past three decades, the Internet of Things (IoT) has evolved from early computing concepts in the 1990s into a commercially mature technological paradigm that enables intelligent and interconnected systems. Although evolutionary models vary, they consistently describe a trajectory from basic device connectivity to increasingly autonomous and intelligent systems. Today, the IoT presents a dual reality: it has reached a level of technological maturity that supports widespread deployment in industry, healthcare, transportation, and agriculture, enabling capabilities that extend from simple identification to predictive maintenance and autonomous decision-making. However, challenges remain, including persistent definitional ambiguity and the absence of unified standards. The article also highlights key research priorities.

**KEY WORDS:** Internet of Things (IoT), Edge Computing, Artificial Intelligence of Things (AIoT), Smart Cities, IoT Security, RFID Technology

### 1. INTRODUCTION

The Internet of Things (IoT) represents one of the most transformative technological paradigms of the 21st century, enabling interconnected devices to communicate, collect data, and make intelligent decisions [5, 11]. This expanding technological ecosystem has reshaped human-environment interaction and unlocked new possibilities for automation, efficiency, and data-driven intelligence across a wide range of sectors. Understanding IoT's historical evolution is therefore essential for anticipating its future development and addressing the challenges that accompany its rapid expansion [13].

This review examines the progression of IoT from its conceptual foundations to its contemporary maturity, highlighting key milestones in its development and identifying

emerging trends that are likely to influence its future trajectory.

### 2. HISTORICAL FOUNDATIONS AND EARLY BEGINNINGS

The evolution of the Internet of Things (IoT) can be traced through a series of defining milestones spanning nearly three decades [19, 20]. Its earliest manifestation is often associated with a modified Coca-Cola vending machine developed at Carnegie Mellon University in 1982, which allowed users to remotely check inventory and temperature—an early glimpse of the connected systems that would later characterize IoT [5, 19].

Conceptual foundations began to take shape when Mark Weiser introduced the idea of ubiquitous computing in 1988, with his seminal article “The Computer for the 21st Century” published in Scientific American in 1991 [17], establishing the philosophical basis

for pervasive digital environments. During the mid-1990s, advancements in sensor technologies and wireless communication provided the essential technological components that would support future IoT systems [11].

A pivotal turning point occurred in 1999 when Kevin Ashton coined the term “Internet of Things”, consolidating previously fragmented ideas into a unified conceptual framework [1, 3]. In the same year, Bill Joy presented his “Six Webs” framework at the World Economic Forum in Davos, which included the concept of device-to-device (D2D) communication — envisioning an internet of sensors distributed across mesh networks to set up urban systems for maximum efficiency [19, 20]. This period also saw academic interest follow shortly thereafter, with the earliest IoT literature published in 2002 by Schoenberger, who first designed the application of IoT in stores, stating that tiny wireless chips enable stores to have eyes [15].

IoT entered the public and institutional spotlight in 2005 with the United Nations ITU report “The Internet of Things,” which articulated the vision of a digitally augmented world that mirrors physical reality [11, 19]. Standardization efforts continued with the approval of the ITU-T Y.2060 recommendation in 2012, followed by the emergence of formal definitions through the IEEE IoT Initiative in 2015, marking growing academic and industrial legitimacy [10, 11].

The 2010s witnessed rapid expansion and integration of IoT technologies across sectors, particularly as IoT converged with industrial robotics, cloud computing, and large-scale data analytics [12, 13]. In recent years, IoT has transitioned from a developing concept into a key component of the future internet, supported by mature hardware, network infrastructures, and intelligent systems [18]. Despite this progress, a universally accepted definition remains elusive due to the field's broad scope and accelerating evolution [5, 11].

### 3. TECHNOLOGICAL MILESTONES AND ENABLING TECHNOLOGIES

Several technological developments proved crucial for IoT's emergence [11, 12]:

The IoT foundation began with the ARPANET in 1969, which created the Internet's backbone [19]. Embedded computing provided essential processing power for IoT devices, while mid-1990s advances in sensor nodes and wireless communication enabled basic device connectivity and sensing [11].

**RFID** (Radio-Frequency Identification) technology was a breakthrough, especially after Kevin Ashton linked it to IoT in 1999 [1, 2, 3]. The *Electronic Product Code* (EPC) enabled unique identification of objects for networked tracking, forming the basis of early IoT applications. The EPC provided a key element for identifying and linking physical objects to networks. These tag-centric solutions formed the basis of the first IoT generation [11, 20].

Key communication protocols arose to support resource-constrained devices, including **IPv6, 6LoWPAN** (IPv6 over Low-Power Wireless Personal Area Networks), and the **CoAP** (Constrained Application Protocol) [11, 12]. Standard protocols like Wi-Fi, Bluetooth, cellular networks, and industrial standards such as Ethernet/IP ensured versatile connectivity [11].

The **Web of Things** (WoT) architecture leveraged web standards for device connectivity and services, while cloud computing provided scalable infrastructure for device virtualization and management [5, 11, 12].

Leading networking technologies — **Information-Centric Networking** (ICN), **Multiple-Input Multiple-Output** (MIMO) systems, **Coordinated Multipoint transmission** (CoMP), **Device-to-Device communications** (D2D), and software-defined networking — enhanced throughput and flexibility. The advent of 5G was pivotal for ubiquitous IoT deployment [12, 18].

Advances in **Artificial Intelligence** (AI), **Machine Learning** (ML), and **Deep Learning** (DL) expanded IoT capabilities by enabling intelligent data processing and autonomous decision-making at both the edge and cloud levels [12, 13, 16]. **Edge computing** further enhanced IoT performance by processing data

near the source, reducing latency and supporting real-time responses [12, 13]. At the same time, the IoT ecosystem grew with the adoption of diverse enabling devices — such as NFC (Near Field Communication) modules, embedded actuators, sensor nodes, and RFID tags and readers — broadening the range of applications and system functionalities [4, 6, 7, 8, 9, 11].

Specialized technologies such as **Unmanned Aerial Systems** (UAS) and **Low-Power Wide Area Networks** (LPWAN, like LoRaWAN) enabled new applications like precision agriculture and large-scale sensor deployments [11, 12].

Collectively, these milestones transformed IoT from foundational concepts to an integrated, scalable ecosystem enabling varied smart applications [11, 13].

#### 4. CURRENT STATE AND KEY APPLICATION DOMAINS

IoT has expanded across numerous sectors through domain-specific adaptations [11, 12, 18].

In industry, the *Industrial Internet of Things* (IIoT) supports automation, predictive maintenance, and robotics integration across manufacturing sectors such as automotive, electronics, and pharmaceuticals [11, 12]. Healthcare applications — ranging from the *Health IoT* to mobile health systems — enable continuous monitoring, telehealth, and AI-driven diagnostics [11, 12]. In transportation, the *Internet of Vehicles* (IoV) underpins intelligent transport systems and autonomous mobility, forming a core component of smart city ecosystems [11, 18].

Agriculture has similarly evolved through IoT-driven precision farming and *Agri-Food 4.0*, integrating RFID, smart sensors, LPWAN technologies, and *Unmanned Aerial Vehicles* (UAV) to improve crop management and resource efficiency [11, 12]. Smart cities leverage IoT for traffic optimization, energy management, waste collection, and public safety while benefiting from 5G, edge AI, and cloud infrastructures for scalable, real-time urban services [18].

Energy systems increasingly rely on IoT-enabled smart grids, smart meters, and AI-

based analytics to support demand response and integration of distributed energy resources [11, 12]. Cross-domain concepts such as the *Web of Things* (WoT) and the *Wisdom Web of Things* (W2T) highlight the growing convergence of IoT technologies, reflecting their expanding role in addressing societal challenges—from climate action to secure and efficient infrastructures [5, 11].

#### 5. FUTURE DIRECTIONS AND EMERGING TRENDS

IoT development is set to accelerate, driven by key technological and societal trends [12, 13]. Massive deployments will rely on Narrowband and Low-Power Wide-Area technologies such as NB-IoT and LTE-M, delivering cost-effective connectivity for vast networks of low-data, energy-efficient devices used in metering, monitoring, and environmental sensing [11, 12].

Digital twins will expand beyond individual assets to model entire infrastructures, cities, and ecosystems, enabling advanced simulation, planning, and optimization far beyond the limits of physical testing [12, 13, 18].

Integration with autonomous systems will deepen, connecting stationary sensors with mobile agents like autonomous vehicles, drones, and robots. Vehicle-to-everything (V2X) communication will play a pivotal role in enhancing coordination, safety, and operational efficiency [12, 18].

The convergence of IoT and quantum computing offers both promise and challenges. Quantum processing could unlock new capabilities in optimization and security analytics, while necessitating quantum-resistant cryptographic methods to safeguard IoT ecosystems [16].

Sustainability will increasingly shape IoT through energy-efficient hardware, eco-conscious deployment strategies, and applications focused on climate monitoring, resource conservation, and circular economy principles [12, 18].

Blockchain and other distributed ledger technologies may strengthen IoT security by providing decentralized trust, data integrity, and automated smart contracts, though their

resource demands must be balanced with IoT device constraints [16].

Neuromorphic computing represents another frontier, with brain-inspired architectures delivering ultra-efficient on-device intelligence — especially valuable for battery-powered edge sensors [12, 13].

Finally, IoT growth will unfold within evolving regulatory and standards frameworks emphasizing interoperability, privacy, security, and environmental responsibility. Global standardization will be critical to sustaining large-scale, interoperable IoT ecosystems [10, 11, 16].

## 6. CHALLENGES AND OPEN RESEARCH AREAS

Despite significant progress, IoT still faces critical challenges that demand sustained, multidisciplinary research [10, 11, 16]. Interoperability remains a major barrier, as diverse devices, communication protocols, and platforms create fragmentation. Advancing universal standards and governance frameworks is essential for seamless integration across heterogeneous systems [11, 14].

Security and privacy vulnerabilities persist due to weak authentication, inconsistent encryption, and the sheer scale of connected devices. Developing unified, scalable security architectures — supporting lightweight cryptography, secure updates, privacy-preserving analytics, and automated threat detection — remains an open research frontier [10, 16].

Managing data at scale is equally challenging. The massive volume of real-time IoT data requires new approaches to distributed processing, efficient storage, data fusion, anomaly detection, and context-aware decision-making to extract actionable insights without overwhelming infrastructure [11, 12, 14].

Resource constraints further complicate system design. Many IoT devices rely on limited energy and computation, driving the need for ultra-low-power hardware, adaptive algorithms, and energy harvesting techniques to extend device lifespan while preserving performance [11, 12].

Scalability and dynamic network management also present unresolved issues. Billions of interconnected devices require robust architectures capable of maintaining quality of service, ensuring fault tolerance, and supporting large-scale coordination [11, 12].

Human and societal factors add additional complexity. Building user trust through transparent data policies, ethical deployment practices, and privacy protection is essential for widespread acceptance. Understanding the human-IoT interaction and designing inclusive, accessible systems remain key research areas [5, 11].

Finally, integrating AI into IoT systems — particularly on constrained or distributed devices — poses significant challenges. Embedding efficient learning, reasoning, and autonomous decision-making at the edge or across federated networks continues to be a demanding technical problem [12, 13, 16].

Addressing these interconnected gaps will require coordinated advances across technical, social, and regulatory domains. Progress in these areas will be crucial for enabling secure, scalable, intelligent, and trustworthy IoT ecosystems in the next generation of digital infrastructure [11, 16, 18].

## 7. CONCLUSION

The Internet of Things has evolved from Kevin Ashton's visionary concept in 1999 to ubiquitous reality, fundamentally transforming how we monitor, understand, and interact with the physical world [1, 3]. Ashton's original insight—that computers should gather information independently through sensors rather than relying on human data entry—has been realized far beyond his initial focus on RFID and supply chain management [2, 3].

The development trajectory reveals progressively sophisticated integration of sensing, communication, computation, and actuation capabilities across expanding application domains [11, 13]. Government investments combined with market valuations underscore IoT's transition from experimental technology to critical infrastructure [18].

Looking forward, IoT's continued evolution will be shaped by technological advances in edge computing and AIoT integration, 5G/6G

network expansion, and artificial intelligence, alongside societal factors including regulatory frameworks, security imperatives, and sustainability requirements [12, 13, 16]. The edge computing market coupled with connected devices generating data at unprecedented rates, indicates that the next phase of IoT development will be characterized by distributed intelligence rather than centralized cloud processing [13].

Security remains paramount, with recent research emphasizing that sophisticated threats—from adversarial AI to quantum computing vulnerabilities—require equally sophisticated solutions including AI-driven anomaly detection, blockchain frameworks, lightweight cryptography, and post-quantum encryption methods [10, 16].

Smart cities represent perhaps the most visible manifestation of IoT's maturation, demonstrating practical benefits in public safety, transportation efficiency, energy management, and quality of life [18]. However, success requires not merely technological deployment but also community engagement, transparent data governance, and sustainable funding models that balance initial capital investments against long-term operational benefits [18].

Success in realizing IoT's full potential requires addressing persistent challenges around security, interoperability, privacy, energy efficiency, and economic viability through coordinated efforts among researchers, industry practitioners, policymakers, and standardization bodies [11, 16]. As IoT systems become increasingly integrated into critical infrastructure and daily life, ensuring their reliability, security, and alignment with human values becomes paramount [5, 11].

The next decade will likely witness IoT transitioning from connecting devices to creating truly intelligent, autonomous environments that anticipate needs, optimize resources, and adapt to changing conditions [12, 13]. This evolution from the "Internet of Things" to an "Intelligence of Things"—or as current research terms it, AIoT—represents not merely technological advancement but a fundamental reimagining of how digital and physical realms interrelate [12, 13]. The vision

Kevin Ashton articulated in 1999, of computers knowing "everything there was to know about things", is becoming reality, though the implications extend far beyond what anyone could have imagined at the millennium's turn [1, 3].

## REFERENCES

- [1] Ashton K., *Internet of Things, presentation at Procter & Gamble*, 1999.
- [2] Ashton, K., *Interview with RAIN RFID Alliance* on IoT vision and RFID evolution, 2015.
- [3] Ashton, K., *That 'Internet of Things' Thing*, RFID Journal, 2009.
- [4] Borcosi I., Gilca G., *Using the touch sensor to control an animatronic platform*, Revista Fiabilitate și Durabilitate Seria, No. 1/2020, ISSN 1844 -- 640X, pag.188-193.
- [5] Chin J., Callaghan V., Allouch S.B., *The Internet-of-Things: Reflections on the past, present and future from a user-centered and smart environment perspective*, Journal of Ambient Intelligence and Smart Environments, 2019.
- [6] Gilcă G., *Applications developed with the objects from the field of Internet of Things*, National Scientific Conference with international participation CONFERENCE 2017, Târgu-Jiu, Dec. 08-09, Nr. 4, 2017, pp. 102-107, ISSN 1842-4856, Annals of the „Constantin Brâncuși” University from Tg. Jiu, Engineering Series.
- [7] Gilcă G., *Smart home system application based on internet of things*, National Scientific Conference with international participation CONFERENCE 2018, Târgu-Jiu, Nov. 23-24, Annals of the „Constantin Brâncuși” University from Tg. Jiu, Engineering Series, No 4, 2018, pp. 101-106, ISSN 1842-4856.
- [8] Grofu F., *Fast Data Acquisition System*, Revista de Fiabilitate și Durabilitate Nr 1/2022 Editura "Academica Brâncuși", Târgu Jiu, ISSN 1844 -- 640X, pg. 49-54.
- [9] Grofu F., Popescu L., *Wind Speed and direction monitor system*, Revista de Fiabilitate și Durabilitate Nr 1/2019

Editura "Academica Brâncuși", Târgu Jiu, ISSN 1844 -- 640X, pg. 244-249.

[10] IEEE Xplore, *IoT Security: Ongoing Challenges and Research Opportunities*, 2014.

[11] Kassab W., Darabkh K., *A-Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations*, Journal of Network and Computer Applications, 2020.

[12] Kinza Shafique, Khawaja B.A., Sabir F., Qazi S., Mustaqim M., *Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios*, IEEE Access, 2020.

[13] Prathyusha M.R., Bhowmik B., *IoT Evolution and Recent Advancements*, 9th International Conference on Advanced Computing and Communication Systems (ICACCS), 2023.

[14] Runcceanu A., *Fragmentation in distributed databases*, International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering Conference, Dec. 3-12, 2007, University of Bridgeport, USA, published in Innovations and Advanced Techniques in Systems, Computing Sciences and Software Engineering, Springer Science, ISBN 978-1-4020-8734-9.

[15] Schoenberger, C.R., *The Internet of Things*, Forbes, March 18, 2002.

[16] Springer Nature, *Internet of Things (IoT) applications security trends and challenges. Discover Internet of Things*, Dec. 2024.

[17] Weiser, M., *The Computer for the 21st Century*, Scientific American, 265(3), pp. 94-104, September 1991.

[18] Zaman, M.; Puryear, N.; Abdelwahed, S.; Zohrabi N.M, *A Review of IoT-Based Smart City Development and Management*, Smart Cities 2024, 7, 1462-1501.

[19] Wikipedia contributors, *Internet of Things*, Wikipedia, The Free Encyclopedia, accessed Nov. 2024.

[20] PMC/NIH, *Tracking the Evolution of the Internet of Things Concept Across Different Application Domains*, accessed Nov. 2024.