Iraqi Journal of Information and Communications Technology(IJICT)
Vol. 9, Issue 1, April 2026
www.ijict.edu.iq
ISSN:2222-758X
e-ISSN:2789-7362

TOWARDS INTELLIGENT CONTROL ARCHITECTURES: A SYSTEMATIC REVIEW OF INTERNET OF THINGS APPLICATIONS IN CONTROL SYSTEMS

Hamzah M. Marhoon[1], Hussein Al-Rammahi[2], Noorulden Basil[3], Nidal Qasem[4], Benmessaoud Mohammed Tarik[5]

[1] Department of Automation and Artificial Intelligence Engineering, College of Information Engineering, Al-Nahrain University, Jadriya, Baghdad, Iraq

[2] Department of Software Engineering, Faculty of Engineering and Architecture, Altinbas University, Istanbul, Türkiye

[3] Department of Electrical Engineering, College of Engineering, Mustansiriyah University, Baghdad, Iraq

[4] Department of Communications and Computer Engineering, Faculty of Engineering, Al-Ahliyya Amman University, Amman, Jordan

[5] Electrical and Electronics Engineering Faculty, University of Sciences and Technology of Oran, USTO-MB, BP 1505, EL M'Naouer, Oran, Algeria

hamzah.marhoon@nahrainuniv.edu.iq[1], hussein.alrammahi1@altinbas.edu.tr[2], noorulden@uomustansiriyah.edu.iq[3], ne.qasem@ammanu.edu.jo[4], tarik.benmessaoud@univ-usto.dz[5]

Corresponding Author: **Benmessaoud Mohammed Tarik**

Received:25/03/2026; Revised:09/04/2026; Accepted:28/04/2026
DOI:10.31987/ijict.9.1.373

***Abstract*- The rapid proliferation of the Internet of Things (IoT) has significantly transformed modern control systems by enabling real-time data acquisition, intelligent decision-making, and seamless connectivity across distributed environments. This paper presents a systematic review of IoT-based control systems, covering studies published between 2015 and 2025, with emphasis on architectural foundations, enabling technologies, control strategies, and major application domains. The review paper analyses five key domains, namely industrial automation, smart manufacturing, healthcare, smart homes and buildings, transportation, and energy and smart grids, while examining major control and optimization approaches integrated with IoT, including data-driven, adaptive, intelligent, and distributed control methods. It also identifies four major cross-cutting challenge categories, namely security and privacy, interoperability and standardization, latency and reliability, and energy efficiency and sustainability, which continue to limit large-scale deployment. In addition, the study highlights eight emerging research directions, including edge-fog-cloud co-design, federated learning, TinyML, digital twins, zero-trust security, and safe learning-based control. The novelty of this review lies in its unified perspective that connects IoT architecture, embedded intelligence, control and optimization frameworks, and cross-domain applications within a single analytical structure. By synthesizing existing literature and revealing key research gaps, this work provides a clearer foundation for developing secure, scalable, and resilient next-generation IoT-driven control systems.**

keywords: **Internet of Things (IoT), Smart Control Architectures, Embedded Systems, Automation, Smart infrastructure.**

I. INTRODUCTION

The Internet of Things (IoT) can be considered one of the significant technological innovations that change the relationship between physical and computerized systems. It can be defined as a system of connected devices that have sensors and actuators and exchange and process data with a minimal number of human interventions [1]. In contrast to conventional technologies that were concentrated on human communication, IoT allows machines to communicate and interact with

ISSN:2222-758X
e-ISSN:2789-7362

humans giving rise to intelligent cyber-physical systems. It is implemented in smart cities, Industry 4.0, digital healthcare, and energy management systems, which are based on this capability [2]. The IoT architecture is usually represented in the form of a layered structure that represents the functionality of the IoT systems. In this regard, the perception layer represents the process of gathering environmental data through sensing technologies, which is then transmitted through the communication networks between the devices. The data is then processed in the middleware layer, in which the intelligent services are performed through the application of the computing function. The application layer represents the process of providing services in different domains like healthcare, industry, and transportation, as represented in Fig. 1. The integration

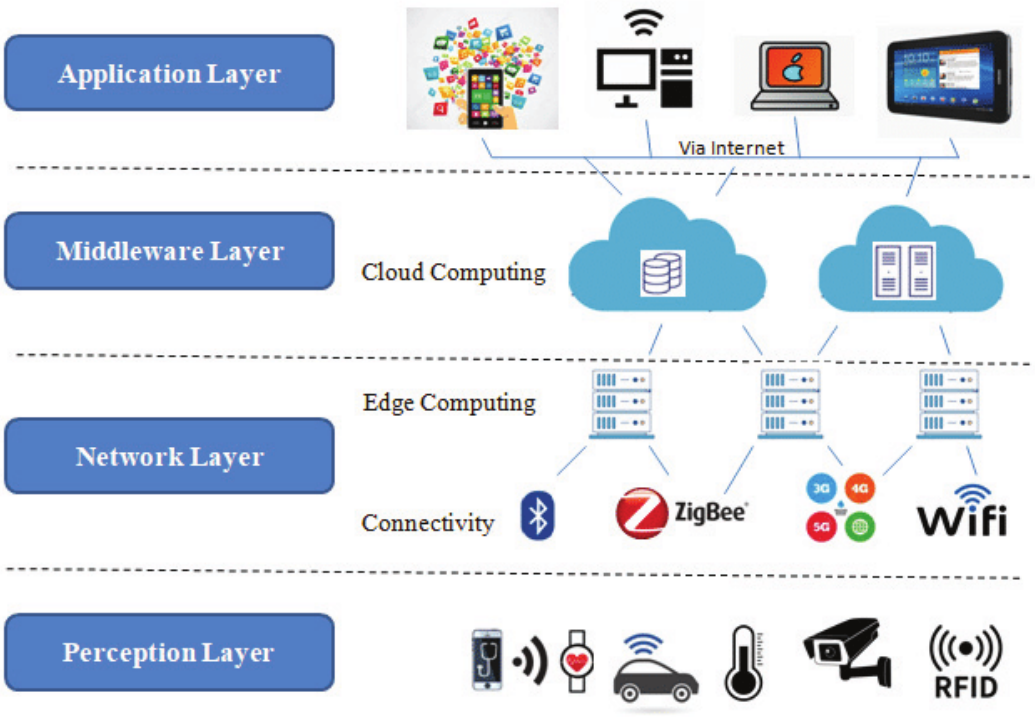

Figure 1: Fundamental segments [5].

of IoT with modern control systems is a paradigm shift in the architecture of control systems [6]. Conventional control systems have been developed around a centralized closed-loop feedback control system, where embedded processors are used for control purposes with the help of sensors and actuators for a particular task or a local operation. Such control systems may prove to be efficient for a particular scenario; however, they may not prove to be flexible or global in their outlook [7]. IoT has taken this a step further with the development of a distributed system consisting of intelligent devices that cooperate with one another for a particular control objective [8]. Such control systems have been developed for efficient monitoring and predictive maintenance in industries [9], continuous patient monitoring and diagnosis in healthcare [10], real-time coordination in transportation systems [11], and home automation in domestic settings [12]. Embedded systems have a crucial role to play in this scenario; however, with the integration of IoT, these systems have evolved beyond their

ISSN:2222-758X
e-ISSN:2789-7362

conventional operation to become a crucial part of a dynamic intelligent control system [13],[14].

With these opportunities and challenges in view, the purpose of the paper is to perform a systematic review of the IoT applications in control and embedded systems and with special emphasis on how the technologies can be used in creation of intelligent control architectures. Investigating the structural models of IoT and their roles and usage, the current research tries to provide an insight into how IoT can revolutionize control systems. Much focus is narrowed to the process of changing control loops with the help of the IoT and how these technologies influence the construction of intelligent control architectures. Through examining these features of IoT and how they have been used in the control and embedded systems, the study will provide contributions to the comprehensive understanding of IoT and how it is poised to revolutionize control systems.

II. Proposed Review Methodology

This paper was done as a systematic review to present a systematic and reproducible study of the use of the IoT in control systems. The major academic databases such as IEEE Xplore, Scopus, ScienceDirect, SpringerLink and Google Scholar were used to conduct the literature search. The review was primarily based on the publications only published in 2015-2025, but some older studies were also included to gain background information when required. The search strategy included the combination of the following keywords: Internet of Things, IoT-based control systems, embedded systems, smart control architectures, industrial IoT, and IoT optimization. The screenings of the collected studies were done in a series of steps, as identification, screening of titles and abstracts, full-text screening and last selection. The articles were added since they had a direct connection with IoT-enabled control systems, embedded intelligence, control or optimization techniques, and key areas of application, including healthcare, industry, smart homes, transportation, and energy systems. The studies were filtered out based on whether they were duplicated, insufficient technical description, and general topics about IoT without specific references to control systems. Then, the chosen papers were analysed and categorized based on their architectural models, enabling technologies, control strategies, application domains and significant challenges. This systematic process contributed to making the literature synthesis clear and assisted in outlining research trends, limitations, and future directions in the area of intelligent control systems based on IoT.

III. Background and Related Work

The growing amount of work on the IoT testifies to its immense importance in the development of infrastructure in modern conditions, especially in the smart control and embedded systems. IoT enhances flexibility, efficiency and scalability by providing continuous monitoring and real-time reaction to dynamic setting. Although there is no unanimity in the method of its implementation, such as prototyping and simulation, overall, there is an agreement on its efficiency in improving the performance and reliability of the system in several applications like home automation, energy management, and healthcare. Serpanos and Wolf (2018) offer models of IoT architecture with the focus on the layered design, security, and system-level factors [15]. Priyadarshini et al. (2023) explore the field of IoT-based healthcare systems, pointing out the trade-offs of the efficiency of the algorithms, energy consumption, and latency in processing ECG [16]. Wu and Chen (2024) suggest a multi-layer IoT control system that will produce lower power usage and will still have a stable output [17].

ISSN:2222-758X
e-ISSN:2789-7362

Following that, Murad, Bayat and Marhoon (2021) implement a two-layer smart house set up based on Arduino and NodeMCU, and an efficient automation, security, and energy efficiency are shown [18]. Kostolani, Murin, and Kozak (2019) discuss the problem of interoperability in the context of industrial applications, where the authors combine the legacy systems of PLCs with the IoT gateway and the Node-RED [19]. Moreover, Tran and Ha (2015) present a decentralized control framework that enhances stability and performance of the system facilitating the reliable IoT-based control systems [20].

The system that Sahrab and Marhoon (2022) suggest involves a low-cost smart home security system based on the Nano and Leonardo microcontrollers, which will include intrusion, fire, and gas sensors and controlled with the help of Bluetooth. The product can be shown to be cost-effective and can perform reliably than GSM- and internet-based ones [21].

Kadhim et al. (2026) value-add an ESP32-based smart medical storage device based on the IoT, supported by Wi-Fi and environmental sensors and surveillance capabilities. The system is highly accurate, consumes little power, and enhances the security of the sensitive medical products [22].

Putra, Akbar, and Ramadhani (2023) develop a smart home system based on Raspberry Pi that can be used to control lighting and temperature through the Blynk application, the work of which is organized in the manual and automatic mode with stable real-time performance [23]. On the same note, Jabbar et al. (2018) introduce Wi-Fi-based home automation system with Arduino Mega and Virtuino app, which can provide cost-effective solution to local and remote control of appliances [24].

The article by Iqal et al. (2024) presents a systematic review of the topic of access control in IoT and examines 96 studies to solve the problem of fragmentation in the field. Their work recognizes important requirements, facilitating technologies, and measures of evaluation, which are useful in achieving a more coherent vision of IoT security [25]. Next, Xu et al. (2018) give a detailed review of the Industrial IoT in the context of Cyber-Physical Systems and connects the control architecture, networking, and computing paradigm. Their work elucidates a trade-off made in the completion concerning the latency, reliability, and growth in the industrial setting [26].

Ganda et al. (2024) give a systematic review of the IoT security, discussing the layered architecture, vulnerabilities and mitigation measures. They note in their work the absence of secure-by-design solutions and the necessity of verifiable and updateable security solutions throughout the IoT stack [27].

Lee, Park, and Kim (2018) introduce a proposal of IoT-powered and AR-assisted disaster management in smart buildings, which combines the multi-sensors and the real-time directions. They show in their prototype that evacuation and situational awareness are more effective in case of an emergency [28].

Alsharif, Kelechi, and Albreem (2024) survey IoT-based monitoring and control systems, in terms of applications, architectures, and communication technologies. They emphasize that it is necessary to choose appropriate communication protocols depending on the specifics of the system and the necessity to guarantee interoperability and high-security systems [29]. Zreikat, Atwan, and Ezdawi (2025) explore the implementation of the IoT at 5G networks, where security issues are discussed concerning a large-scale environment with low latency. They draw attention to the purpose of AI-driven detection schemes and secure OTA updates to guarantee robust IoT deployments [30].

ISSN:2222-758X
e-ISSN:2789-7362

Kobara et al. (2016) analyze cybersecurity threats to IoT and industrial control systems and single out weak authentication and exposure through such tools as SHODAN. They suggest a multi-level defense framework such as network isolation, credential management, and security testing tools and provide an effective guidance on protecting the systems [31].

In the article, Alshdadi (2023) introduces an IoT-oriented smart home assistant that serves as a self-care system applicable to the elderly population group. The proposed KNN-ABC model is much more efficient compared with the conventional approaches as it enhances the activity recognition and brings about greater user safety [32].

Dhaou et al. (2023) create an IoT-based smart meter and plug-based system to monitor the energy in real-time, allowing the precise measurements of electrical parameters and the automated reaction (turning on the load, turning off the load) to the specific incidents and shows the successful energy management in the homes [33].

Kurniyawani (2025) develops a privacy-conscious smart home security solution which incorporates motion and on-device AI and mobile apps. The system offers real-time alerts without sacrificing responsiveness and privacy factors [34].

Soliman et al. (2017) suggest a low-cost IoT-based home automation and security system with the usage of Raspberry Pi and wireless sensors. Their system allows real-time monitoring and access remotely and they prove to be very reliable and efficient in working practices [35]. Kotha and Gupta (2018) consider the IoT applications, architectures, and enabling technologies, noting some of the fundamental issues, including interoperability and security in smart environments [36].

Neelakandan et al. (2021) suggest the IoT-based traffic control system on optimized OWENN classifier with high accuracy and enhanced adaptive traffic signal control [37]. The survey of Sikder et al. (2018) of IoT-enabled smart lighting systems indicates that they can help to save energy by up to 33.33 percent [38].

Samie et al. (2016) consider embedded computing in IoT focusing on design trade-offs regardless of resource constraints and enabling the creation of low-power and secure edge devices [39]. Netinant et al. create a multimodal IoT home automation system, which is reliable in voice and sensor-based control and its performance is maintained [39]. Alsharif, Alzahrani, and Alotaibi (2020) present a smart waste management system, which is an IoT-based platform that works with sensor-based bins to monitor waste parameters in real-time, enhancing its efficiency and safety in urban settings [40]. Kaza et al. (2018) also highlight the importance of data-driven approaches and governance systems in streamlining large-scale waste management systems [41].

Finally, Alam, Reaz, and Ali (2012) cover a review of the smart home technologies in details, stating the challenges like security and interoperability and the advantages they have on energy efficiency, automation and quality of life [42].

In Table I, major IoT research between 2015 and 2025 has been summarized. Early studies were on control structures and simple home automation, but later studies were on industrial interoperability, energy efficiency, and security. By 2021-2022, the focus changed to low-cost smart systems and traffic management based on such platforms as Arduino and Raspberry Pi. The latest researches implement the most innovative methods of machine learning and AI in order to improve performance, privacy, and real-time flexibility. In general, these trends underscore the future of IoT and present a basis to the further development of research directions.

ISSN:2222-758X
e-ISSN:2789-7362

TABLE I
Summary of IoT applications and research contributions (2015–2025)

Authors	Year	Contribution	Method	Results
Serpanos & Wolf	2018	IoT architecture models	Device–fog–cloud layered design	Improved scalability and system organization
Priyadarshini et al.	2023	ECG IoT healthcare	FPGA-based QRS detection	High accuracy, low power (∼0.7 mW)
Wu & Chen	2024	Energy-efficient IoT control	Multi-layer + gateway protocols	Reduced energy consumption, stable output
Murad et al.	2021	Smart home security	Arduino + NodeMCU, sensors	Reliable automation and intrusion detection
Kostoláni et al.	2019	Industrial IoT gateway	Siemens IoT2040 + Node-RED	Improved interoperability and scalability
Tran & Ha	2015	Decentralized control	DepCS/DSC framework	∼35% performance improvement
Sahrab & Marhoon	2022	Low-cost smart home	Dual microcontrollers + sensors	Affordable and reliable system
Marhoon et al.	2023	Vehicle safety system	GSM/GPS + sensors	Real-time tracking and alerts
Putra et al.	2023	Raspberry Pi smart home	Sensors + Blynk app	Low-cost, responsive control
Jabbar et al.	2018	Wi-Fi home automation	Arduino Mega + app	Practical remote-control system
Iqbal et al.	2024	Access control survey	Systematic review	Identified research gaps
Xu et al.	2018	IIoT/CPS survey	Layered system analysis	Clarified design trade-offs
Ganda et al.	2024	IoT security review	Layered threat analysis	Highlighted security challenges
Lee et al.	2018	IoT–AR disaster system	Sensors + AR interface	Improved evacuation efficiency
Alsharif et al.	2024	IoT systems survey	Cross-domain analysis	Emphasized interoperability needs
Zreikat et al.	2025	IoT–5G integration	AI security + OTA updates	Enhanced resilience and security
Kobara et al.	2016	ICS/IoT security	Layered defense + honeypots	Practical security improvements
Alshdadi	2023	Elderly smart home	KNN–ABC + robot	∼93.7% accuracy, improved safety
Dhaou et al.	2023	Energy management	Smart meter/plug + IoT	Real-time monitoring and control
Kurniyawani	2025	AI home security	PIR + camera + ML	Privacy-aware real-time alerts
Soliman et al.	2017	Smart home system	Raspberry Pi + cloud	Reliable, low-latency monitoring
Kotha & Gupta	2018	IoT survey	Applications + architecture	Identified key challenges
Neelakandan et al.	2021	Traffic control	OWENN classifier	∼98% accuracy, reduced congestion
Sikder et al.	2018	Smart lighting	Sensor-based IoT	∼33% energy savings
Samie et al.	2016	Embedded IoT systems	HW/SW co-design	Efficient low-power systems

Netinant et al.	2024	Voice-based smart home	IoT + voice/PIR sensors	High accuracy & reliability
Alsharif et al.	2020	Smart waste system	Sensor-based IoT bins	Improved efficiency and safety
Kaza et al.	2018	Waste management	Data-driven systems	Enhanced urban sustainability
Alam et al.	2012	Smart home review	Architecture + communication	Improved automation and QoL

IV. Evolution of IoT

IoT development is closely connected with the advance of industrial revolutions. Industry 1.0 was marked by the mechanization and Industry 2.0 was marked by electricity and mass production. Industry 3.0 was typified by automation and utilization of digital technologies. The industry 4.0 integrates IoT and cybers-physical technologies, AI, as well as sophisticated networking and establish intelligent connectivity (see Fig. 2). The IoTT in its essence may be regarded as the outcome of the long-term industrial innovation that has resulted in the development of interconnected, autonomous physical things.

The dynamism of the number of IoT devices highlights its transformational nature to the industry and society. It is estimated

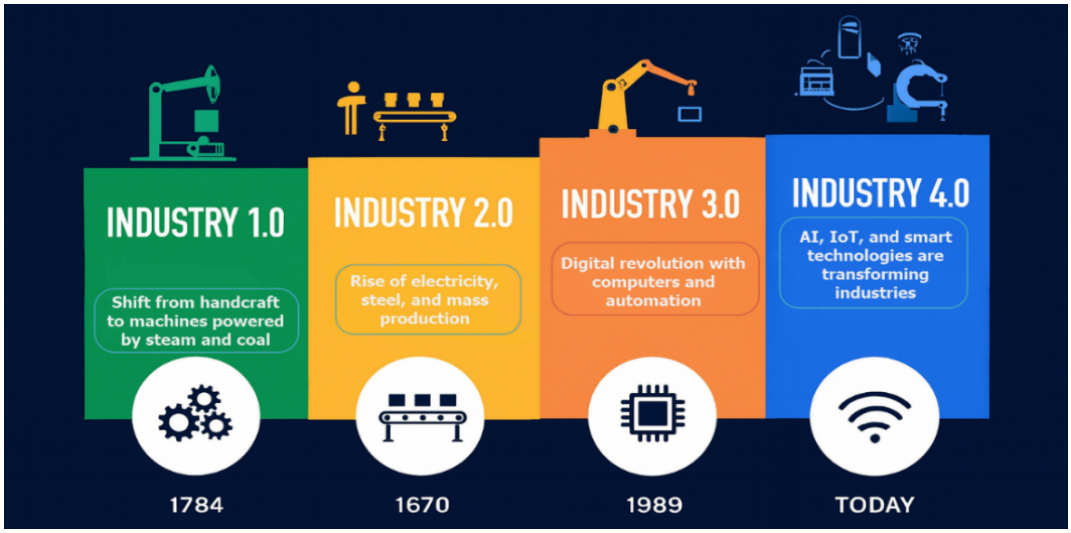

Figure 2: Industrial revolutions from mechanisation to IoT.

that the number of connected devices in the world will grow as a result of an average yearly growth of 16.6 billion in 2019 up to 25.2 billion in 2028 (Fig. 3). True impetus behind this growth includes sensor miniaturization, IPv6, and low-latency 5G networks where real-time communication is possible [44]. Also, edge computing helps to diminish the use of centralized systems as it can perform local data processing, which enhances responsiveness. IoT systems have become predictive and autonomous in their decision making coupled with artificial intelligence and machine learning. Therefore, IoT has become a necessity in areas like precise agriculture, healthcare, smart grids, and smart transportation systems [45].

ISSN:2222-758X
e-ISSN:2789-7362

The following Fig. 4, provides an example of the layered IoT architecture in which the perception, communication, and

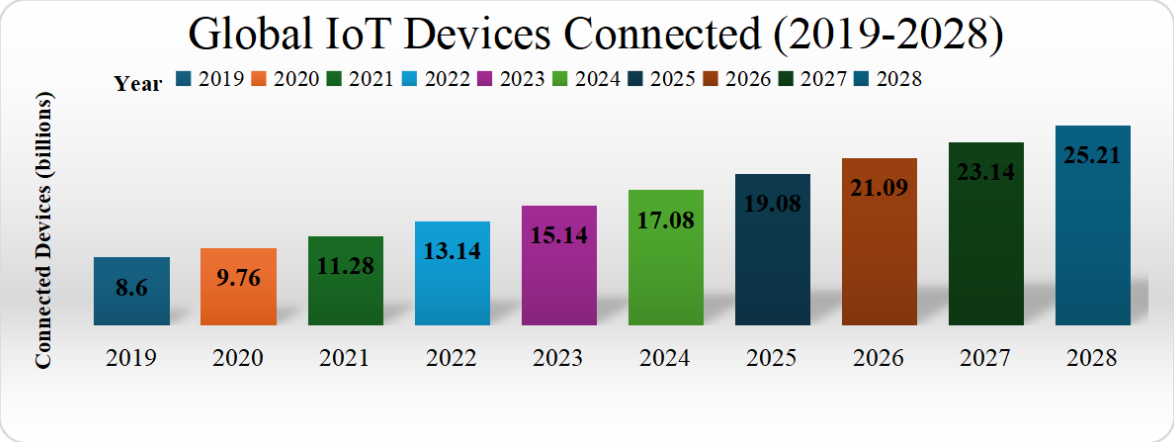

Figure 3: Global IoT device growth (2019–2028).

computation aspects can be integrated to enable the smooth interaction of the physical and digital worlds in different fields of applications including healthcare, industry, and smart cities. The perception layer entails gathering and transformation of the environment by sensors that underlies the measurement of accuracy and dependability of the system. Data can be transmitted using many technologies depending on the network layer including Wi-Fi, Bluetooth, and 5G, hence, ensuring interoperability and real-time communication. Data storage, processing, and analysis, which are facilitated by cloud or edge computation, are part of the application layer hence creating knowledge to make decisions. The IoT market has been witnessing a considerable growth all over the world with projections going up to USD 260 billion in 2019 to around USD 835 billion in 2028 (Fig. 5) and is currently undergoing one of the highest growth rates in the ICT sector. Some of the developments that have facilitated this growth include low-power wide-area networks, the uptake of 5G, the miniaturization of sensors, and the combination of AI and machine learning with edge computing [47, 48]. The pace of the post-2020 boom is partly associated with the COVID-19 pandemic, which hastened the implementation of the IoT in the fields of telemedicine, remote monitoring, and automation. This trend is consistent with diffusion of innovation theory and network externalities, in which more people being connected makes a system valuable. Although it is growing, there are still issues such as standardization, cybersecurity, energy efficiency and governance. In general, IoT is a significant part of Industry 4.0 that defines the future technological and socio-economic systems [49].

V. IoT Foundations in Control and Embedded Systems

The integration of the Embedded systems may be regarded as the core of the IoT as it is the computational and control core that connects physical and digital space. An IoT device generally comprises of an embedded system which contains sensors, actuators and processing devices to measure real world data and run automated actions. Fig. 6 demonstrates that sensors and actuators are connected to the environment and send their data to the embedded devices, including medical systems, smart meters, or industrial controllers, to be processed and controlled [50]. This is followed by attaching

ISSN:2222-758X
e-ISSN:2789-7362

Figure 4: Layered IoT architecture for smart data acquisition and cloud integration (redrawn and adapted from [46]).

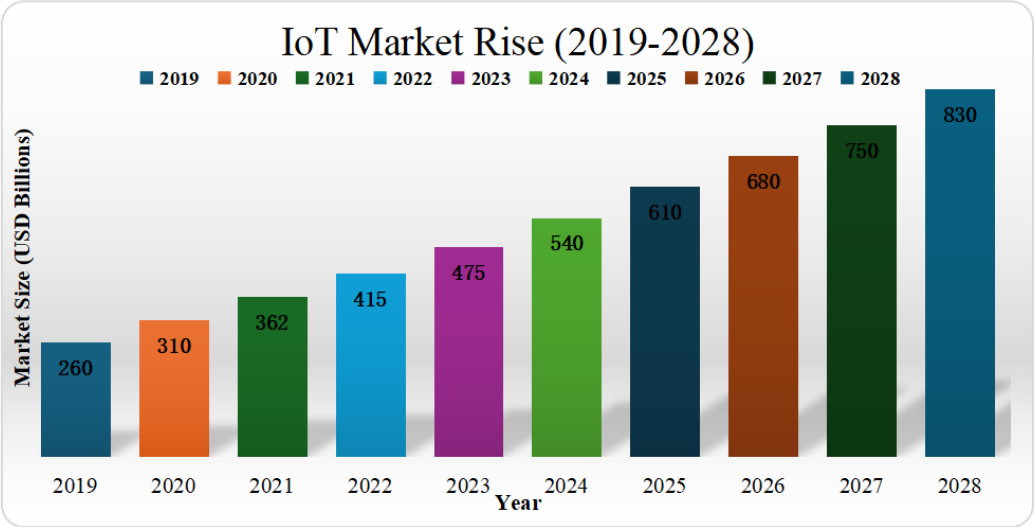

Figure 5: Global IoT market growth and projections from 2019 to 2028.

these embedded systems to a communication infrastructure either via a local network (e.g. home router) or a wide area cellular network enabling real-time exchange of data with a server and distributed platforms over the web. This top-down

ISSN:2222-758X
e-ISSN:2789-7362

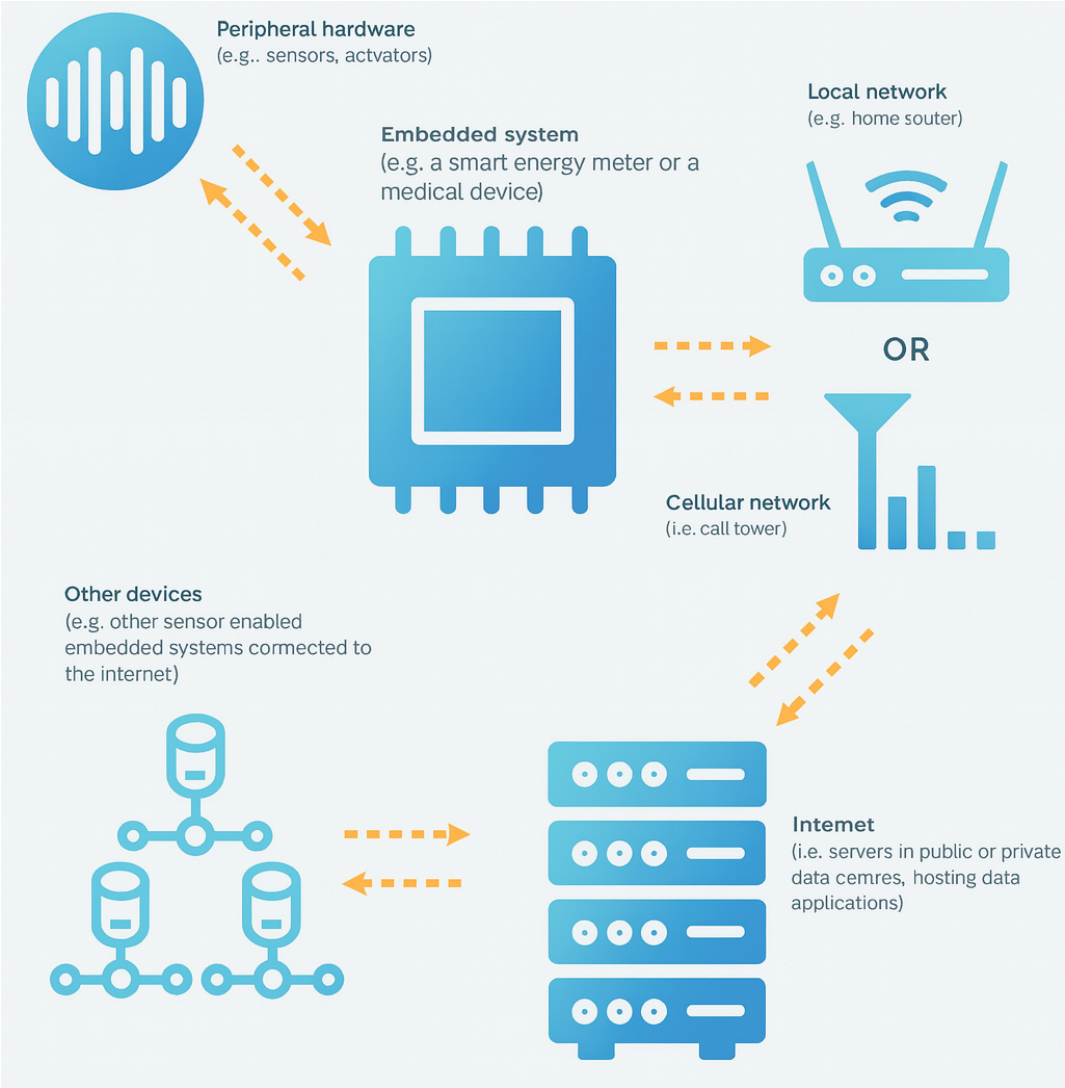

Figure 6: IoT embedded systems interacting with hardware, networks, and the internet.

connectivity is an indication that embedded systems cannot function in isolation but are a part of a larger ecosystem of interconnected devices that form the IoT. Continuing on this, Fig. 7 displays the general structure of the IoT whereby the IoT devices are linked to the gateways running either embedded or real-time operating systems which transmit data over the networks and cloud infrastructure to the application platforms [51]. This pipeline is indicative of the layered IoT architecture which has device, gateway, network, cloud and application layers with each layer adding to overall intelligence of the end-to-end system. Embedded systems can be deployed to serve as local controllers, allowing fast decision-making locally without cloud-based optimization and coordination analytics. Their low power consumption coupled with real-time performance capabilities make them very necessary in critical applications like the healthcare, autonomous systems and

ISSN:2222-758X
e-ISSN:2789-7362

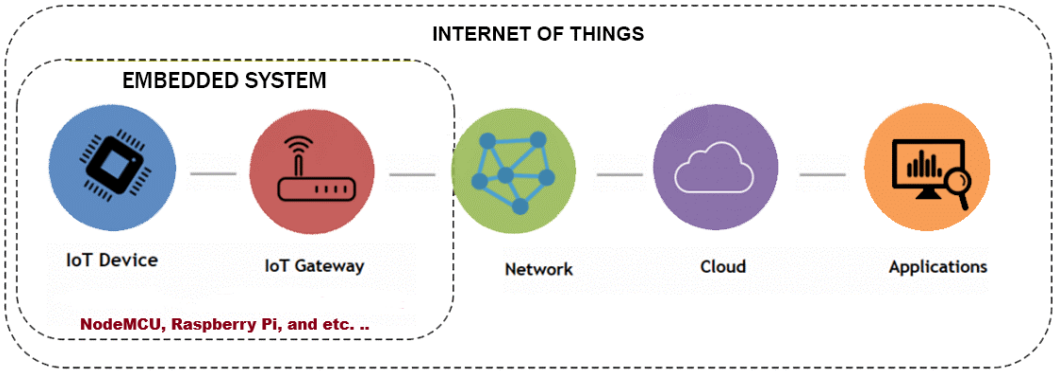

Figure 7: Simplified IoT architecture.

industrial automation. Together with enhanced sensing and trusted communication, scalable data management, embedded systems constitute the basis of the IoT as a functional cyber-physical ecosystem in tune with the industry 4.0 [52]. The IoT is also the paradigm shift of the control systems as it shifts the centralized architectures to the distributed intelligence. The IoT allows the local decision-making of edge devices, in contrast to traditional systems that are susceptible to latency and single points of failure, so that global coordination is achieved through cloud or fog computing. It is applicable in applications like smart manufacturing and energy systems to improve real time control, system efficiency and resilience [53], [65]. Besides, the IoT leads to the development of control theory, making systems adaptive and predictive, which enhances their performance and fault tolerance. On the whole, it changes control systems into self-organizing adaptive networks in such industries as healthcare, transportation, and agriculture [54].

VI. Application Domains of IoT in Control Systems

The fast development of the IoT has transformed the outlook of the current state of control systems by incorporating intelligence, connectivity, and information-based decision-making in a broad range of areas of application. In contrast to the control architectures of the old times that were centralised and inflexible, the IoT-enabled systems are based on distributed sensing, embedded computation, and real-time communication to form adaptive, resilient, and context-aware infrastructures. All these functions enable IoT to address the disparity between tangible processes and digital ecosystems through the conversion of unprocessed sensor data into operational knowledge by using edge intelligence, sophisticated communication systems, and cloud-based data management. IoT has brought about innovation in the modern socio-technical systems by being efficient, flexible, and sustainable. Its influence can be traced in various settings, different industries and energy plants, healthcare systems, transport systems, and houses. In order to underline such a range of influence, five key areas where IoT has a critical role in the contemporary control are discussed in the following subsections industrial automation and smart manufacturing, healthcare and biomedical systems, smart homes and buildings, transportation and mobility, and energy and smart grids.

ISSN:2222-758X
e-ISSN:2789-7362

A. Industrial Automation and Smart Manufacturing

The integration of IoT into industrial automation and smart manufacturing represents a significant shift aligned with Industry 4.0, combining cyber-physical systems, connectivity, and data-driven intelligence. Modern systems adopt a multi-layered architecture where sensors, gateways, and cloud services interconnect to form integrated industrial ecosystems (see Fig. 8). Smart IoT sensors enable real-time monitoring of parameters such as temperature and vibration while supporting historical data analysis for predictive maintenance and process optimization [55].

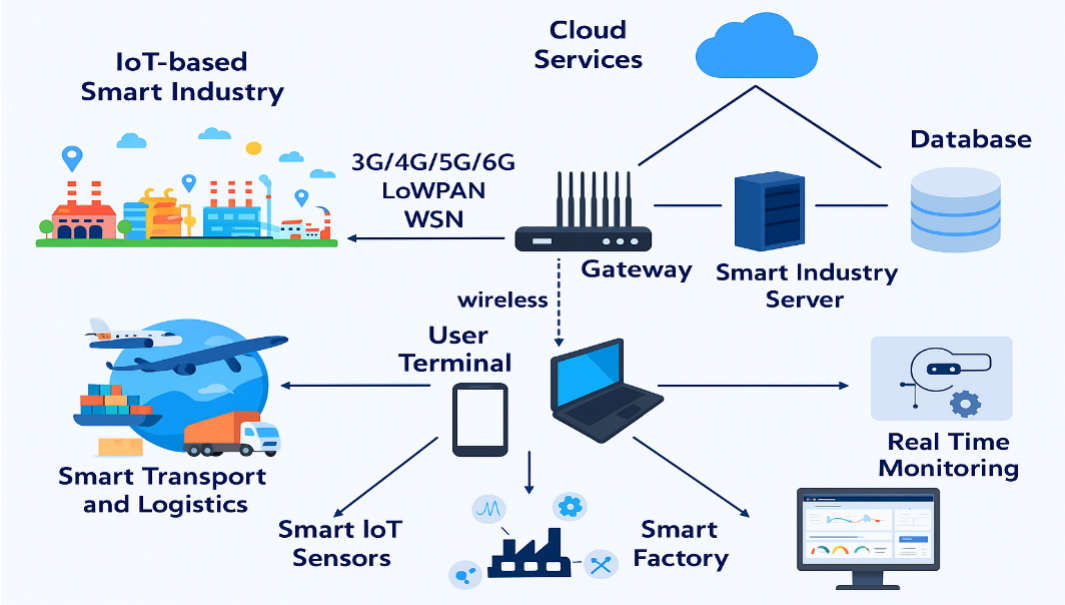

Figure 8: IoT ecosystem in smart industry applications.

The IIoT architecture (Fig. 9) is grounded on six interconnected layers, i.e. physical processes and data acquisition, data processing, and data analysis. The physical level of interaction is possible due to the use of sensors, actuators, and microcontrollers, and the interoperability is achieved by communication protocols like ZigBee, LoRaWAN, Wi-Fi, MQTT, and CoAP. The processed data is calculated through computation instruments to assist predictive maintenance, energy optimization, and adaptive control [56]. IIoT also allows cross-domain applications, and it can be used to support machine-to machine communication, asset monitoring, and flexible manufacturing. It is compatible with SCADA systems, and this feature improves monitoring and semi-autonomous operations. Also, IIoT can be used to make an organization more sustainable through the saving of energy and increasing equipment maintenance time. Nevertheless, there are still issues, such as scalability, information protection, and cyber-physical resistance [57].

ISSN:2222-758X
e-ISSN:2789-7362

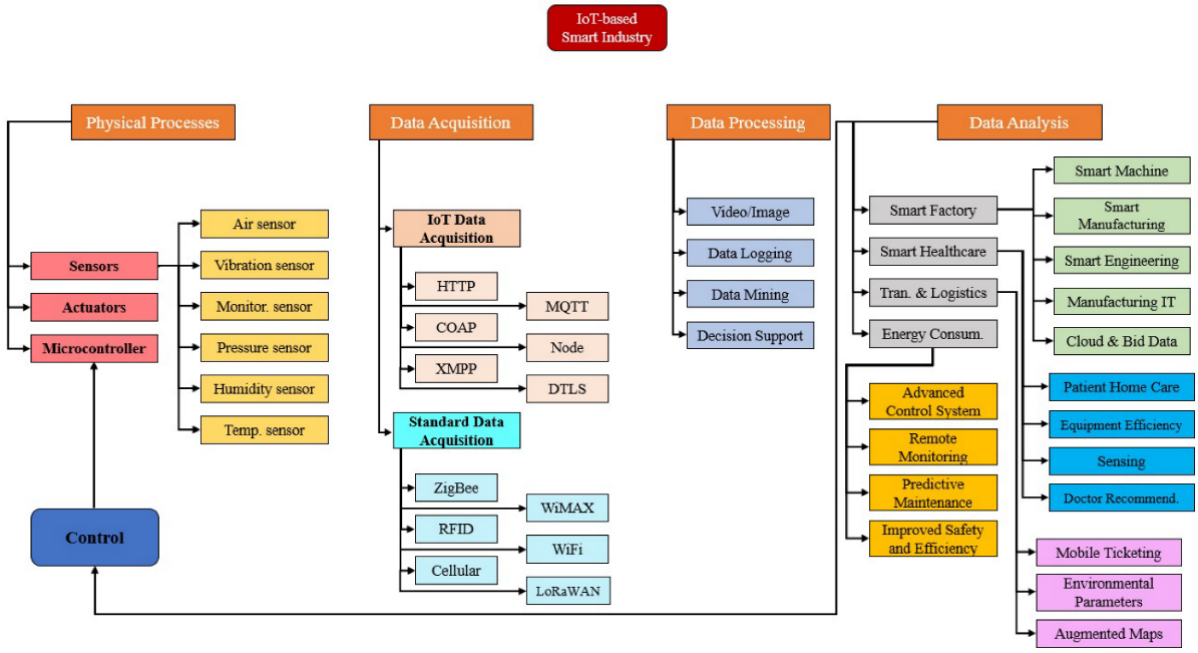

Figure 9: Architecture of IoT-enabled industrial automation [56].

B. Smart Manufacturing

The IoT and IIoT have a major role to play in facilitating smart manufacturing in Industry 4.0. Whilst IoT is a general term used to relate devices, IIoT is applied to the industrial settings where efficiency, reliability, and productivity are of paramount concern. It allows real-time machine, sensor, and enterprise systems communication, and supports more advanced strategies, including predictive maintenance, intelligent scheduling, and adjustive production. Compared to conventional automation, IIoT supports interrelated, agile, and robust manufacturing, and is also compatible with other technologies like AI, big data, and cyber-physical systems [57], [58].

The fundamental building blocks that constitute IIoT are embedded systems and especially microcontrollers that offer real-time and low-cost processing and communications. They connect physical machines to digital platforms allowing them to monitor and control on a continuous basis. As an example, smart manufacturing involves microcontrollers reading sensor readings of equipment and sending the readings to be analysed, which helps predict the maintenance and optimize the process. Through IoT, IIoT, and adjacent technologies, including cloud computing and AI, which is shown in Fig. 10, smart factories can become adaptive, data-driven, and self-optimizing systems [59].

C. Healthcare and Biomedical Systems

The application of IoT and embedded systems especially microcontroller-based systems has greatly improved the current healthcare applications through real-time monitoring and decentralized decision making. Implantable and wearable gadgets gather physiological information, which is computed locally and can be sent through low power communication technologies

ISSN:2222-758X
e-ISSN:2789-7362

Figure 10: IoT and enabling technologies of the smart factory within Industry 4.0.

to gateways like smartphones. These gateways send the data to the cloud systems, making clinicians to be able to conduct remote monitoring, diagnosis and intervention. Application areas include telemedicine and mobile health which are supported by this layered architecture and make care continuity and scalability more achievable (see Fig.11). In systems terms, it is a transition to cyber-physical healthcare settings which will improve efficiency, access and patient-centred care [60]. Microcontrollers are also important in facilitating local intelligence in the healthcare systems based on IoT because they allow real-time processing, including signal filtering and emergency response. This is edge-level processing that minimizes latency and bandwidth usage as well as provides reliable operation even at network failure. It also enables constant monitoring of patients and anomalies can be identified at an early stage and medical care taken. On a bigger scale, IoT and microcontroller-based systems enable optimization of healthcare on a large scale, such as resource management and AI-based diagnostics. These technologies, combined, are accelerating the process of implementing efficient, connected and patient-focused healthcare systems [61].

D. Smart Homes and Buildings Systems

Smart homes and buildings are one of the most important applications of IoT, which will turn the traditional environment into smart, efficient, and responsive systems. These systems are usually three-layered in architecture, i.e. perception, network and application. Data about the environment and operation are gathered using sensors and processing and control is made possible through embedded systems, thus minimizing the latency, and making it possible to respond to events in real time. Information is sent through communication systems including Wi-Fi and ZigBee to cloud systems, which produce insights and automate activities in a closed-loop system using AI and machine learning [62]. Such architectures

ISSN:2222-758X
e-ISSN:2789-7362

Figure 11: IoT-enabled smart hospital architecture.

maximize energy efficiency, security and comfort to the user. As an example, occupancy- and environment-responsive lighting and HVAC systems can be used, and security systems connected to the IoT can deliver real-time data and alerts. Embedded microcontrollers can guarantee good local performance even when there are connectivity problems and predictive maintenance since they can detect possible system failures [63]. Smart homes are not only isolated structures but they also form part of larger smart city systems, where they communicate with energy grids, transport and health systems. Such interconnectedness can facilitate sustainable management of resources and city-level resilience, and IoT-enabled buildings (see Fig. 12) have become the key constituents of smart cities and Industry 4.0 infrastructures in the future [64].

ISSN:2222-758X
e-ISSN:2789-7362

Figure 12: IoT-enabled smart building ecosystem.

E. Transportation and Mobility Systems

The IoT and embedded systems and the enhanced communication technologies are changing the transportation and mobility systems in a radically different manner and are all elements of safer, more efficient and sustainable mobility. The contemporary smart transportation systems are way ahead of car monitoring, and have since been expanded to include cars, buses, and trains, aeroplanes and water transport as coherent and intelligent systems. These systems rely mostly on the IoT devices and embedded microcontrollers that collect data through cameras mounted on the cars, roads and transit stations and process it locally to make decisions in real time and transfer them to communication systems to be analysed on large scales. The intelligent mobility architecture depicted in Fig. 13 takes into account an enormous variety of different elements: adaptive cruise control and vehicle to vehicle communication systems that reduce the number of collisions and maximize the driving efficiency; fleet management systems that observe the situation and optimize the logistics; and the platforms that regulate the navigation that adjusts to the situation on the road. On the same note, the crash avoidance and travel assistance programs incorporate the use of microcontrollers to decode the resultant data brought about by the cameras, radars, and lidar systems to produce a real-time response to avoid accidents [65]. Besides road transport, intermodal coordination, in the context of IoT-based communication networks (e.g. WLAN, mobile networks, land-based broadcast and satellite networks), involves the connection between the various forms of travel (e.g. trains, buses, ships and aeroplanes) into a mobility chain. One of them is passenger information systems which can offer real-time arrival and departure, interconnection, and trip-planning services which can incorporate this information into convenient applications in order to make the commuters more comfortable. The indicators and intelligent infrastructure developed using the IoT may be applied in the traffic management to respond dynamically to the traffic, weather, or emergency to reduce traffic jams and

ISSN:2222-758X
e-ISSN:2789-7362

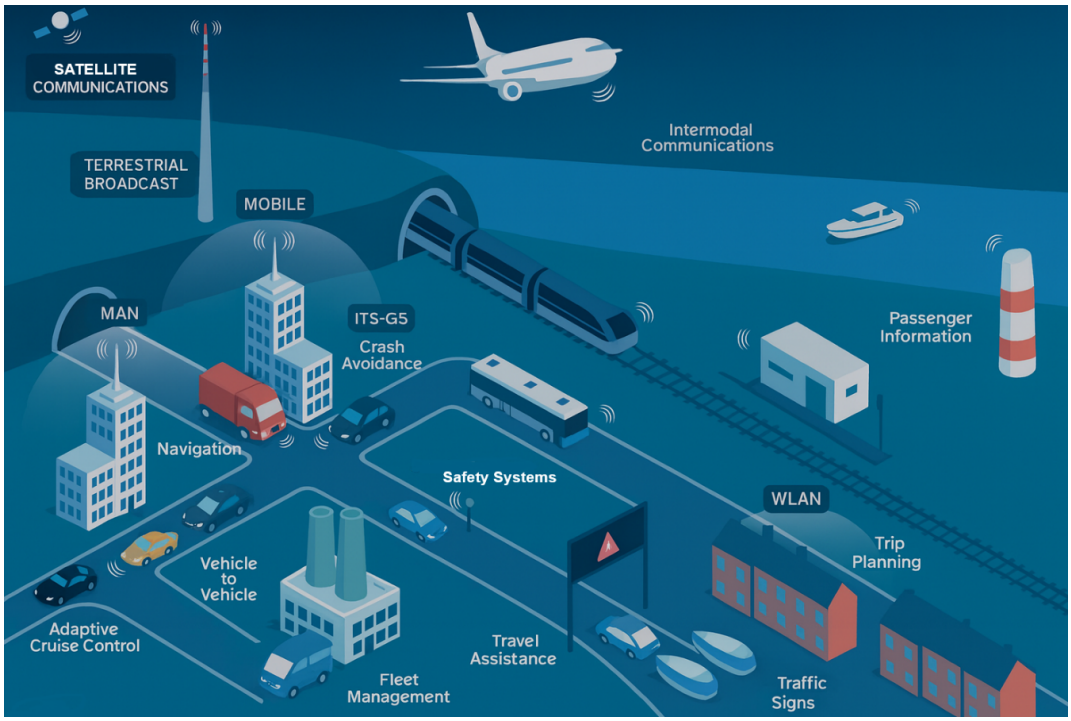

Figure 13: IoT-enabled smart transportation and mobility system.

become one of the factors that increase the degree of urban safety. Infrastructure embedded systems and automotive ensure that edge-safe and rapid data processing is performed to reduce the latency time of critical safety processes. Meanwhile, a more advanced set of applications like predictive analytics, demand forecasting and transport network optimisation can be implemented on cloud-based platforms. The mixture of the above may be viewed as a paradigm shift of mobility as it is no longer an individual vehicle that is being automated through the assistance of IoT and embedded systems; it is an entire multimodal transport networks that are being planned. Subsequently, there is an influential use of intelligent transportation systems in building sustainable cities, prevention of accidents, enhancement of the efficiency of the environment, and it offers people and goods with consistent mobility [66].

F. Energy and Smart Grids Systems

Introduction of the IoT and the IIoT to energy systems and smart grids is an evolutionary revolution occurring in the current infrastructure of power generation, and is, in essence, the restructure of the production, transmission, distribution, and consumption of electricity. The Internet of Energy (Fig. 14) provides an example of how, based on interconnected devices, modern communication systems, and intelligent data processing, a cyber-physical ecosystem brings together households, industries, electric vehicles, renewable energy plants, and utility operators [67]. At the consumer end, IoT-based applications, such as smart meters, home energy management systems and smart appliances are adopted to offer granular real-time consumption feedback to prosumers to enable them to maximise their energy use, and participate in demand response

ISSN:2222-758X
e-ISSN:2789-7362

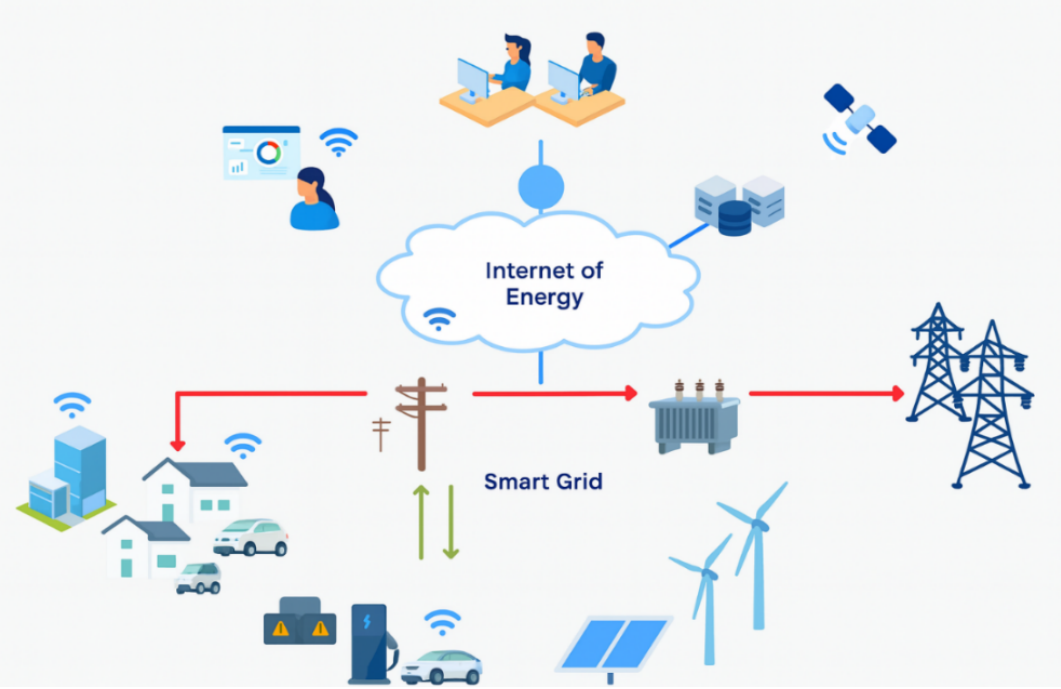

Figure 14: Integration of IoT and IIoT within the internet of energy and smart grid ecosystem.

programmes. At the industrial level, IIoT scenarios maximise the efficiency of significant objects, including transformers, substations and renewable energy farms, through predictive maintenance, fault detection, and autonomous control, reduce downtimes and ensure that the life cycles of the objects are as long as possible. The combination of the distributed renewable energy sources and intelligent forecasting algorithms and dynamic grid-balancing systems with IoT and IIoT nodes will enable the integration of such sources and will enable overcoming the challenges of the intermittency of the given resources. In addition, the two-way communication of the smart grids enables the potentiality not only of load balancing, but also of peer-to-peer energy trading that makes possible the existence of decentralised energy markets and micro grid architectures. The supportive infrastructure takes advantage of the cloud computing, edge computing, and satellite-aided communication to compute large amounts of heterogeneous data securely and with low latency to offer both cyberspace resilience and operational reliability. Such kind of the ecosystem can be predicted by the application of predictive analytics to it by bringing machine learning and artificial intelligence to it to predict consumption patterns, optimise storage space in batteries and electric vehicles, and minimise losses in transmission across the network. The synthesis between the structure of IoT and IIoT in the Internet of Energy forms an adaptable, scalable, self-governing energy model that is capable of responding to the exigencies of sustainability, grid resilience, and a carbon emission reduction and a crucial step towards the realisation of smart, sustainable cities and decarbonised energy futures of the global energy transition models [68].

ISSN:2222-758X
e-ISSN:2789-7362

VII. IoT-Enabled Control and Optimisation Frameworks

IoT-based control and optimization systems have converted the classical inflexible control systems into flexible, layered, cyber-physical system that brings together sensing, communication, computation and actuation at edge, fog, and cloud layers. Fast local control is supported by real-time information obtained by distributed sensors, whereas the coordination, optimization, and large-scale analytics are maintained by fog and cloud layers. Metaheuristics and other advanced optimization methods are common in the tuning of controllers as well as allocation of resources in complex constraints [83-85]. Adaptive control under uncertainty can be achieved using decision-making techniques including fuzzy logic, Bayesian inference, and reinforcement learning, which are frequently used as a combination of model-based and data-driven techniques. Federated and distributed learning also feature greater system scalability, privacy and resilience against uncertainties and attacks are also improved by robust and stochastic optimization. Also, formal verification techniques provide stability and safety of the systems. Together, these will allow static, robust, and self-organizing IoT control systems in complicated real-world systems [69, 70]. Having a mission with the aim of integrating IoT in the control and optimization systems provides a platform where intelligent systems are able to confront complex, uncertain and dynamic environments. IoT devices generate enormous volumes of data which are exposed to edge, fog, and cloud computing to enable real-time and long-term decision-making. The metaheuristic algorithms and decision-making processes i.e. reinforcement learning and Bayesian methods is what enables predictive maintenance, resource optimization and adaptive control. The various optimization models like the PSO, Genetic Algorithms and the Grey Wolf Optimization offer various methods of parameter tuning and system design and hence are more scalable and resilient in cases of critical application [71-76]. These frameworks are also assisted by embedded systems since they combine digital intelligence and physical processes. Cheap systems include PIC microcontrollers, Arduino, and Raspberry Pi that may be utilized to gather data, process it onboard, and manage devices. They are also flexible and scaled and can be incorporated with the communication networks and cloud systems to facilitate effective and reliable deployments of IoT. Brought together, the technologies will be able to bridge the theoretical-practical disconnect in such fields as smart grids, transportation and factory automation [77, 78].Table II summarize the optimization and decision-making algorithms for IoT-based control systems.

VIII. Cross-Cutting Issues and Challenges

The ubiquity of IoT-based control systems is curtailed by diverse intersective issues that directly determine their reliability, credibility and long-term scalability. The most urgent concerns are always found to be security and privacy, surveys show that vulnerable issues such as unauthorised access, data alteration, and cyberattacks are some of the major hindrances, and these issues are cited by about 49 percent of the respondents. The necessity of ensuring a good data integrity, implementation of strong authentication mechanisms, and implementation of intrusion-detection systems is therefore a major precondition of mission-critical infrastructures. The interoperability and standardisation issues which the nearly 36% of the questionnaire respondents reported about are also vital due to the difficulty of integrating heterogeneous devices and communication protocols into the multi-vendor environment. Without standardisation, interoperability gaps emerge causing inefficiencies and limiting the scale of the massive IoT solutions. The next burning problem is linked to energy

ISSN:2222-758X
e-ISSN:2789-7362

TABLE II
Optimization and decision-making algorithms for IoT-based control

Algorithm	Type	IoT Control Use	Advantages	Limitations
PSO	Swarm	PID/MPC tuning, routing, energy	Fast, simple, parallel	Premature convergence, parameter-sensitive
GA	Evolutionary	Network design, task allocation	Flexible, multi-objective	High cost, encoding dependent
HHO	Swarm	Parameter tuning, prediction	Strong exploration	Slow convergence
Jaya	Parameter-free	Edge control tuning	No parameters, lightweight	May stagnate
BH	Physics	Routing, clustering	Simple, balanced search	Diversity loss
AOA	Physics	Scheduling, energy optimization	Handles constraints well	Limited validation
ROA	Swarm	Multi-agent coordination	Adaptive	Parameter sensitivity
GWO	Swarm	Controller tuning	Few parameters, global search	Slow exploitation
COA	Swarm	Fault detection, routing	Escapes local optima	Computationally heavy
SFO	Swarm	Clustering, coverage	Efficient distribution	Limited theory
MPC	Model-based	Energy, control, coordination	Predictive, constraint-aware	Model-dependent, heavy
BO	Surrogate	Hyperparameter tuning	Sample efficient	Poor scalability
Fuzzy / Fuzzy MPC	Rule-based	Uncertainty handling	Interpretable, robust	Rule explosion
ADMM / Distributed Opt.	Distributed	Multi-agent systems	Scalable, privacy-aware	Needs reliable comms
POMDP	Probabilistic	Decision under uncertainty	Handles partial info	High complexity
MCDA (AHP, TOPSIS, PROMETHEE)	Decision-making	Multi-objective trade-offs	Transparent	Needs weights

efficiency and sustainability, which nearly fifty three percent of the respondents cite as a critical concern especially in the resource-starved environment where miniature-power gadgets and extended networks is a compulsory provision. This ought to be solved through developing energy gathering inventions, energy conservation communication protocols and developing green IoT systems which are eco-friendly. The barriers to adoption could be also central and one-third of the respondents reported reliability and safety as the barriers to adoption, especially in mission critical applications like healthcare monitoring, industrial automation and smart grids where failures even in the short-term can be disastrous. The operation of variable and safety must be redundant, formally verified and fault-tolerant control systems which are controlled in an adaptive manner. These problems described in Fig. 15, are characterized by varying amounts of reported research but when added together, they indicate that technical advances in the IoT-enabled control should be facilitated by answers to systemic risks and the lack of clarity in its functioning. It is only after these dimensions are solved that the IoT-based control systems would be robust, scalable, and reliable, which is essential in a real-life system [79, 80].

ISSN:2222-758X
e-ISSN:2789-7362

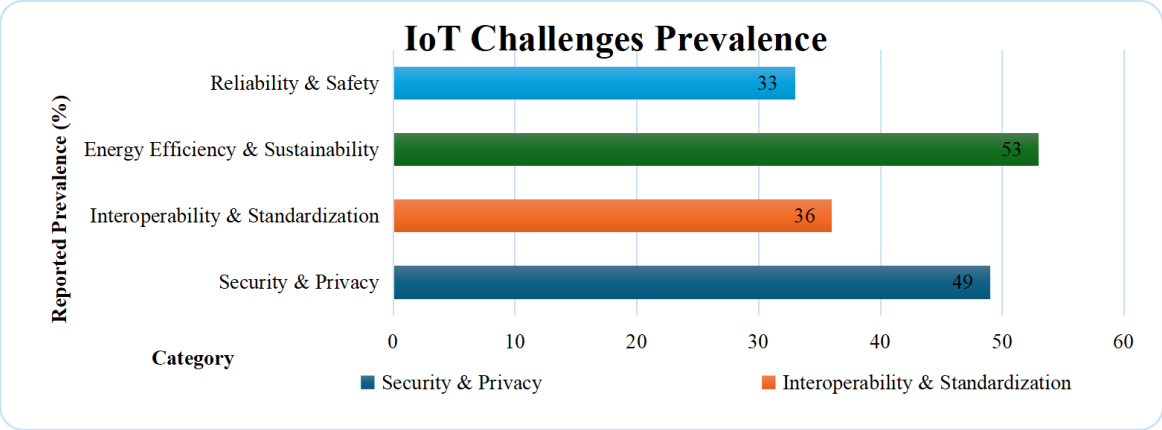

Figure 15: Documented prevalence of cross-cutting challenges in IoT-based control systems.

IX. Emerging Trends and Research Directions

New studies in the field of control systems based on the IoT underline a number of directions. Co-design Edge-fog-cloud allows the distributed control with the allocation of real-time tasks to edge layers and global optimization to the cloud in order to minimize latency and bandwidth consumption [81]. URLLC innovations over 5G/6G guarantee high reliability and low delay time-sensitive applications [82], whereas federated learning contributes to privacy via the decentralized model training approach [83]. Also, TinyML enables on-device intelligence to enhance robustness and digital twins can be used to simulate and provide predictive control using data-driven models in real-time [84], [85]. Zero-trust and blockchain-based strategies enhance security whereas safe reinforcement learning and distributed optimization techniques can enhance performance, safety, and scalability [86], [87]. These trends are summarized in Table III and are associated with the IoT control stack and their functions in distributed architectures, communication efficiency, privacy-preserving intelligence, and real-time decisions. Other methods that contribute to greater reliability and adaptability of the system include digital twins, consensus optimization, and learning-augmented control. Together, these advancements offer a blueprint to scalable and secure as well as resilient IoT-oriented control systems in the real-world complex settings [88].

Fig. 16 highlights the growth of IoT-enabled smart control domains between 2023 and 2025. Smart homes show steady growth, increasing from USD 118.9 billion to USD 147.5 billion, driven by demand for automation and energy management. Smart cities represent the largest and fastest-growing segment, rising from USD 679.8 billion to USD 894.1 billion due to infrastructure expansion and sustainability initiatives. In contrast, smart irrigation grows modestly from USD 1.47 billion to USD 1.59 billion, reflecting its niche role in precision agriculture. Smart transportation also shows gradual growth, reaching USD 58.3 billion by 2025 through advancements in connected and intelligent transport systems. Overall, these trends demonstrate both large-scale and sector-specific contributions of IoT to efficiency and sustainability across domains [102, 103].

ISSN:2222-758X
e-ISSN:2789-7362

TABLE III
Emerging trends and research directions for IoT-based control systems

References	Trend	Enabling Role in Control Systems	Representative techniques / examples
[89]	Edge–fog–cloud co-design	Push latency-critical loops to edge/fog; use cloud for fleet-level optimization and planning; reduce backhaul and response time	Edge MPC; event-triggered control; dynamic function placement/orchestration
[90]	URLLC (Ultra-Reliable Low-Latency Communication, 5G→6G) for networked control	Millisecond-class latency and "five-nines" reliability for time-critical, remote actuation in industrial/energy systems	Packet duplication (3GPP Rel-16); network slicing; joint communication–control scheduling
[91], [92]	FL for IoT control/analytics	Continual model/policy updates without sharing raw data; privacy and bandwidth efficiency across heterogeneous devices	Federated Averaging (FedAvg); client selection; personalization; anomaly detection; predictive maintenance
[93], [94]	TinyML / on-device inference	Always-on perception and lightweight decision policies on microcontroller units; resilience when offline; reduced backhaul	Quantization; pruning; neural architecture search for MCUs; CMSIS-NN/TVM-micro toolchains
[95], [96]	Digital twins for smart grids & energy	Closed-loop sim-to-control: asset health, DER orchestration, contingency analysis; real-time validation	Physics-/data-driven or hybrid twins; live synchronization with IoT data streams
[97], [98]	Zero-trust & blockchain-backed IoT security	Continuous identity verification; least-privilege access; tamper-evident actuation/data logs	Zero-trust policy engines; lightweight cryptography; distributed ledger for access control and auditing
[99], [100]	Safe RL & learning-augmented MPC	Constraint-aware adaptation with guarantees; safety wrappers for learned policies; RL-tuned MPC	Control-barrier and Lyapunov-based safety layers; safe exploration; RL-assisted MPC adaptation
[101]	Distributed/consensus optimization for multi-agent control	Scalable coordination and estimation with bandwidth/privacy limits; plug-and-play across agents	Consensus protocols; gradient tracking; ADMM and variants; distributed economic dispatch

ISSN:2222-758X
e-ISSN:2789-7362

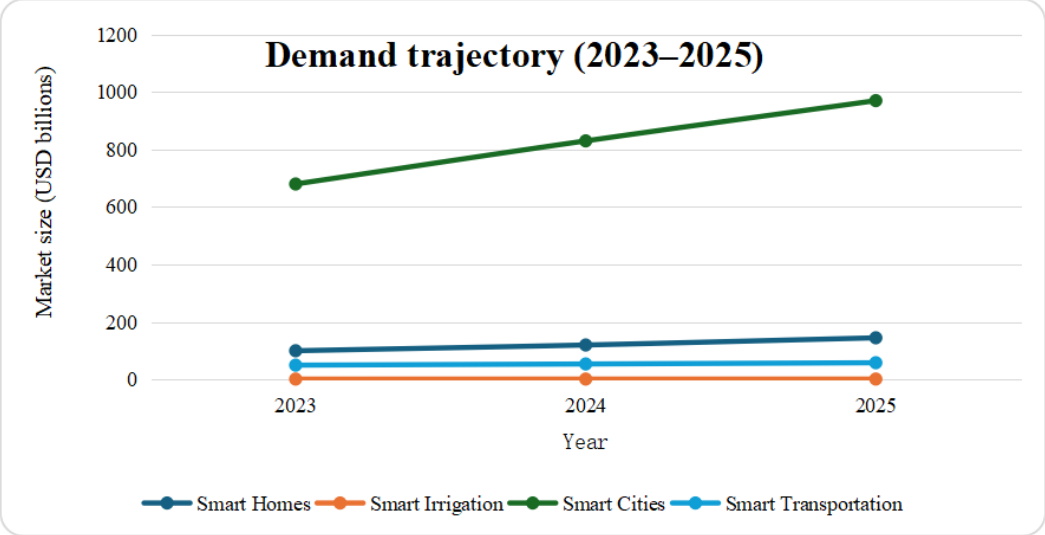

Figure 16: Projected IoT market demand (2023–2025) across smart control domains.

X. Discussion

A cross-domain analysis indicates that the evolution of IoT-based control systems varies according to sector-specific constraints, infrastructure readiness, and regulatory factors (Fig. 17). Smart cities exhibit rapid scalability supported by advanced networks and distributed architectures, while smart homes face challenges related to interoperability and privacy, addressed through approaches such as federated learning and TinyML. Smart irrigation emphasizes energy efficiency and on-device processing, whereas intelligent transportation systems prioritize reliability and low-latency control using advanced optimization and communication technologies. Across domains, three key insights emerge: the importance of multi-layer integration for balancing latency and resilience, the need for built-in security and governance mechanisms, and the shift toward hybrid learning-based control methods. Overall, IoT systems are transitioning from centralized models to distributed, data-driven, and secure architectures, where communication, computation, and control are jointly optimized to ensure performance, scalability, and sustainability in real-world applications [104, 105]. Despite the consistent evidence of the advantages of the IoT implementation in the control systems provided in the reviewed studies, a critical comparison of the articles reveals some significant differences in maturity, scalability, and practicability of the solutions in various domains. An example is smart home or healthcare applications, which are commonly tested by low-cost prototypes and small-scale deployments, proving their feasibility but not necessarily generalizable to large-scale real-world deployments. By contrast, automation in industries and smart grid research are more inclined to use more organized architectures and optimization-based control structures, but have stricter requirements concerning interoperability, cybersecurity and reliability. The other critical inconsistency is that numerous studies have reported accuracy improvement, responsiveness or energy efficiency, but with a variety of measures of evaluation, experimental environments, and hardware platforms, it is hard to compare and contrast. Moreover, although AI- and edge-enabled is also suggested as a solution to adaptive and intelligent control,

ISSN:2222-758X
e-ISSN:2789-7362

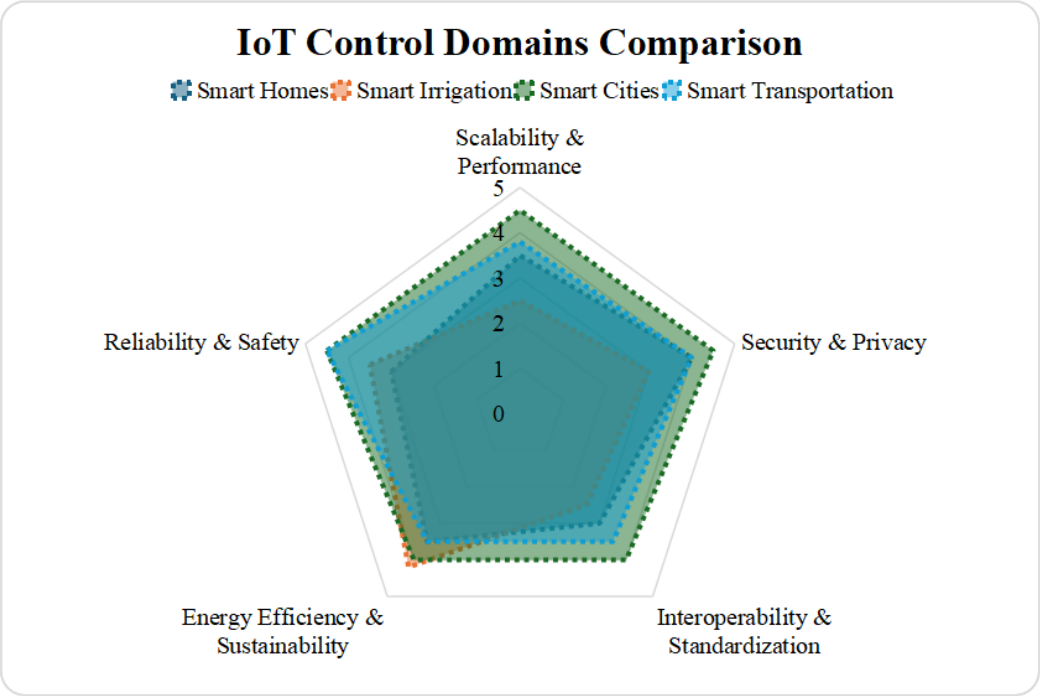

Figure 17: Comparative profiles of IoT control domains.

their sustainable operation, explainability, and safety in mission-critical contexts are not sufficiently proven. This shows that application-specific implementations are abundant in the literature, but still are lacking in the unification of benchmarking frameworks, standard evaluation criteria, and large-scale comparative validation, which are also the main research gaps in future development of IoT-based control systems.

XI. Future Insight for IoT-Based Smart Systems

The future of smart systems using IoT is not only influenced by the development of improved connectivity and intelligence, but also many research gaps that remain unaddressed to date, which restrict the implementation of smart systems on a large scale and reliability. Nevertheless, there remains a gap in the literature of standardized benchmarking frameworks, small-scale real-world validation, inadequate interoperability among heterogeneous platforms, and insufficient security, privacy, and safety-by-design mechanisms. Moreover, despite the growing number of reports on AI-based IoT control approaches, their explicability, stability, and reliability in mission-critical settings are under-investigated. These limitations are critical to the process of enhancing prototype-level implementations to scalable and reliable smart systems. In line with this, a number of significant future directions can be identified. Digital twins and predictive autonomy will help and assist in real-time simulation, predictive maintenance, and adaptive optimization of systems via virtual copies of physical assets. Low-latency, secure communication of critical IoT applications can be enhanced by zero-trust architecture and state-of-the-art 6G-enabled connectivity. Creating sustainable IoT design will continue to be a significant focus, and

ISSN:2222-758X
e-ISSN:2789-7362

the importance of energy harvesting, low-power embedded design, and environmentally friendly operation will continue to increase. IoT systems that are human-centred and ethical are also required to enhance transparency, trust, inclusivity, and pragmatic acceptance of explainable AI-based control. Lastly, cognitive and self-organizing IoT systems offer an exciting future where distributed intelligence can support adaptive, collaborative and self-healing behaviour in complex control systems. In general, the activities of the future research must be aimed at the creation of the intelligent IoT-based smart systems that will be not only intelligent and autonomous, but also secure, interoperable, scalable, explainable, and sustainable [106-110].

XII. CONCLUSION

During the last decade, the growing interaction between IoT and control engineering has redefined how modern systems operate, communicate, and adapt. This review paper has shown that IoT technologies are no longer peripheral tools, but have become central elements in the design of intelligent and distributed control architectures. Through their integration with embedded systems, IoT platforms allow machines, sensors, and software to work together in real time, improving precision, reliability, and response capacity in a variety of applications from industrial automation and health monitoring to transport networks and intelligent energy systems. Based on previous studies that have been published between 2015 and 2025, this review covered six major application domains and highlighted reported quantitative gains, including nearly 35% performance improvement in decentralized IoT-based control systems, about 33.33% energy savings in smart lighting applications, approximately 93.7% accuracy in elderly smart-home assistance systems, and around 98% accuracy in IoT-based traffic control systems. The collected research emphasizes that this progress is driven by advances in sensing, wireless communication, and lightweight edge computing. Nevertheless, despite these achievements, many obstacles remain.

The review identified four major cross-cutting challenge categories, with reported prevalence values of 53% for energy efficiency and sustainability, 49% for security and privacy, 36% for interoperability and standardization, and 33% for reliability and safety. To address these challenges, stronger international standards, more efficient hardware design, and the integration of secure and adaptive algorithms are required to ensure safe operation in complex, data-rich environments. In addition, the review highlighted eight major emerging research directions, including federated learning, TinyML, digital twins, zero-trust security, and edge–fog–cloud cooperation, which are expected to shape the next stage of IoT-based smart systems. Together, these findings suggest a future in which control systems are not only intelligent and autonomous, but also scalable, secure, energy-conscious, and self-improving. In this sense, IoT-enabled control represents more than a technological upgrade; it marks a conceptual shift toward systems that learn, predict, and cooperate within the broader ecosystem of Industry 4.0. As research continues to mature, these architectures will play a decisive role in shaping the future interaction between physical and digital worlds.

FUNDING

None.

ACKNOWLEDGEMENT

The author would like to thank the reviewers for their valuable contribution in the publication of this paper.

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] Al-Dulaimy, M. Jansen, B. Johansson, A. Trivedi, A. Iosup, M. Ashjaei, and A. V. Papadopoulos, "The computing continuum: From IoT to the cloud," Internet of Things, vol. 27, p. 101272, 2024. doi: 10.1016/j.iot.2024.101272.
[2] A. Choudhary, "Internet of Things: a comprehensive overview, architectures, applications, simulation tools, challenges and future directions," Discover Internet of Things, vol. 4, no. 31, 2024. doi: 10.1007/s43926-024-00084-3.
[3] M. Lombardi, F. Pascale, and D. Santaniello, "Internet of Things: A general overview between architectures, protocols and applications," Information, vol. 12, no. 2, p. 87, 2021. doi: 10.3390/info12020087.
[4] N. Freitas, A. D. Rocha, and J. Barata, "Data management in industry: concepts, systematic review and future directions," Journal of Intelligent Manufacturing, 2025. doi: 10.1007/s10845-025-02570-z.
[5] H. M. Marhoon, A. I. Alanssari, and N. Basil, "Design and implementation of an intelligent safety and security system for vehicles based on GSM communication and IoT network for real-time tracking," Journal of Robotics and Control (JRC), vol. 4, no. 5, pp. 708–718, 2023. doi: 10.18196/jrc.v4i5.19652.
[6] Y. Lisboa, L. Santos, E. Lobato, W. Fonseca, K. Silva, I. Rodrigues, and M. Silva, "Design and Implementation of a Sustainable IoT Embedded System for Monitoring Temperature and Humidity in Photovoltaic Power Plants in the Amazon," Sustainability, vol. 17, no. 6, p. 2347, 2025. doi: 10.3390/su17062347.
[7] N. Basil, A. F. Mohammed, B. M. Sabbar, et al., "Performance analysis of hybrid optimization approach for UAV path planning control using FOPID-TID controller and HAOAROA algorithm," Scientific Reports, vol. 15, p. 4840, 2025. doi: 10.1038/s41598-025-86803-4.
[8] Z. H. Ali and H. A. Ali, "Towards sustainable smart IoT applications architectural elements and design: opportunities, challenges, and open directions," Journal of Supercomputing, vol. 77, pp. 5668–5725, 2021. doi: 10.1007/s11227-020-03477-7.
[9] K. Varalakshmi and J. Kumar, "Optimized predictive maintenance for streaming data in industrial IoT networks using deep reinforcement learning and ensemble techniques," Scientific Reports, vol. 15, p. 27201, 2025. doi: 10.1038/s41598-025-10268-8.
[10] M. M. H. Mia, N. Mahfuz, M. R. Habib, and R. Hossain, "An Internet of Things Application on Continuous Remote Patient Monitoring and Diagnosis," in Proc. 4th Int. Conf. Bio-Engineering for Smart Technologies (BioSMART), Paris / Créteil, France, 2021, pp. 1–6. doi: 10.1109/BioSMART54244.2021.9677715.
[11] J. Tripathy, M. Kaliappan, G. K. Chellathevar, J. R. F. Raj, R. Shanmugasundaram, M. Alagarsamy, et al., "Integrating Blockchain and IoT with Advanced Predictive Modeling for Energy Efficient Urban Transportation Systems," Sustainable Computing: Informatics and Systems, 2025, Art. no. 101208. doi: 10.1016/j.suscom.2025.101208.
[12] S. FakhrHosseini, C. Lee, S. H. Lee, et al., "A Taxonomy of Home Automation: Expert Perspectives on the Future of Smarter Homes," Information Systems Frontiers, vol. 27, pp. 449–466, 2025. doi: 10.1007/s10796-024-10496-9.
[13] H. Omrany, K. M. Al-Obaidi, M. Hossain, et al., "IoT-enabled smart cities: a hybrid systematic analysis of key research areas, challenges, and recommendations for future direction," Discover Cities, vol. 1, p. 2, 2024. doi: 10.1007/s44327-024-00002-w.
[14] L. P. Rachakonda, M. Siddula, and V. Sathya, "A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in Next-Generation networks (5G/6G/beyond)," High-Confidence Computing, vol. 4, no. 2, p. 100220, 2024. doi: 10.1016/j.hcc.2024.100220.
[15] D. Serpanos and M. Wolf, Internet-of-Things (IoT) Systems: Architectures, Algorithms, Methodologies. Cham, Switzerland: Springer, 2018. doi: 10.1007/978-3-319-69715-4.
[16] R. Priyadarshini, N. Shaikh, R. K. Godi, P. K. Dhal, R. Sharma, and Y. Perwej, "IoT-based power control systems framework for healthcare applications," Measurement: Sensors, vol. 25, p. 100660, 2023. doi: 10.1016/j.measen.2022.100660.
[17] M. Wu and X. Chen, "Application of Internet of Things and embedded technology in electronic communication," Measurement: Sensors, vol. 34, p. 101246, 2024. doi: 10.1016/j.measen.2024.101246.
[18] M. Murad, O. Bayat, and H. M. Marhoon, "Design and implementation of a smart home system with two levels of security based on IoT technology," Indonesian Journal of Electrical Engineering and Computer Science, vol. 21, no. 1, pp. 546–557, Jan. 2021. doi: 10.11591/ijeecs.v21.i1.
[19] M. Kostoláni, J. Murín, and Š. Kozák, "An effective industrial control approach," in Proc. Federated Conf. Computer Science and Information Systems (FedCSIS), Leipzig, Germany, 2019, pp. 911–914. doi: 10.15439/2019F187.
[20] T. Tran and Q. P. Ha, "Dependable control systems with Internet of Things," ISA Transactions, vol. 59, pp. 303–313, 2015. doi: 10.1016/j.isatra.2015.08.008.
[21] A. A. Sahrab and H. M. Marhoon, "Design and fabrication of a low-cost system for smart home applications," Journal of Robotics and Control (JRC), vol. 3, no. 4, pp. 409–414, 2022. doi: 10.18196/jrc.v3i4.15413.
[22] A. F. Kadhim, A. E. Hamzah, M. A. Al-Shareeda, K. A. Hashim, N. M. Sapiee, H. H. Qasm, et al., "Design and implementation of an accurate and simple remote medical store monitoring system using ESP32 microcontroller-based Wi-Fi and IoT technology," Applied Mechanics and Materials, vol. 934, pp. 63–73, 2026, doi: 10.4028/p-S8LbYh.
[23] U. A. A. Putra, L. A. S. I. Akbar, and C. Ramadhani, "Smarthome design using Raspberry Pi 3 based on Internet of Things (IoT)," SITEKIN: Jurnal Sains, Teknologi dan Industri, vol. 22, no. 2, pp. 280–294, 2022. doi: 10.24014/sitekin.v22i2.37496.
[24] W. A. Jabbar, M. H. Alsibai, N. S. S. Amran, and S. K. Mahayadin, "Design and implementation of IoT-based automation system for smart home," in Proc. Int. Symp. Networks, Computers and Communications (ISNCC), Rome, Italy, 2018, pp. 1–6. doi: 10.1109/ISNCC.2018.8531006.
[25] Z. M. Iqal, A. Selamat, and O. Krejcar, "A comprehensive systematic review of access control in IoT: Requirements, technologies, and evaluation metrics," IEEE Access, vol. 12, pp. 12636–12654, 2024. doi: 10.1109/ACCESS.2023.3347495.
[26] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on Industrial Internet of Things: A cyber-physical systems perspective," IEEE Access, vol. 6, pp. 78238–78259, 2018. doi: 10.1109/ACCESS.2018.2884906.
[27] D. Ganda, R. Chhikara, P. S. Mehra, and D. Chawla, "A systematic review on Internet of Things (IoT) security: Applications, architecture, challenges and solutions," in Proc. 1st Int. Conf. Advanced Computing and Emerging Technologies (ACET), Ghaziabad, India, 2024, pp. 1–8. doi: 10.1109/ACET61898.2024.10729954.

[28] H. S. Lee, S. H. Park, and J. H. Kim, "Development of an IoT-based smart building system for fire detection and evacuation," IEEE Access, vol. 6, pp. 48246–48257, 2018, doi: 10.1109/ACCESS.2018.2869916.
[29] M. A. Alsharif, M. Kelechi, and M. A. Albreem, "Internet of Things (IoT): A review of monitoring and control systems," Sensors, vol. 24, no. 3, p. 939, 2024, doi: 10.3390/s24030939.
[30] A. I. Zreikat, Z. AlArnaout, A. Abadleh, E. Elbasi, and N. Mostafa, "The integration of the Internet of Things (IoT) applications into 5G networks: A review and analysis," Computers, vol. 14, no. 7, p. 250, 2025, doi: 10.3390/computers14070250.
[31] K. Kobara, "Cyber physical security for industrial control systems and IoT," IEICE Trans. Inf. Syst., vol. 99, no. 4, pp. 787–795, 2016, doi: 10.1587/transinf.2015ICI0001.
[32] A. Alshdadi, "Evaluation of IoT-based smart home assistance for elderly people using robot," Electronics, vol. 12, no. 12, p. 2627, 2023, doi: 10.3390/electronics12122627.
[33] I. B. Dhaou, "Design and implementation of an Internet-of-Things-enabled smart meter and smart plug for home-energy-management system," Electronics, vol. 12, no. 19, p. 4041, 2023, doi: 10.3390/electronics12194041.
[34] E. S. Soegoto, B. N. Meliala, S. Luckyardi, and B. Kurniawan, "Computer science research in Indonesia to create sustainable infrastructure for United Nations sustainable development goals," J. Eng. Sci. Technol., vol. 20, no. 3, pp. 670–685, 2025.
[35] M. Soliman, T. Abiodun, T. Hamouda, J. Zhou, and C.-H. Lung, "Smart home: Integrating Internet of Things with web services and cloud computing," Future Generation Computer Systems, vol. 76, pp. 315–326, Nov. 2017, doi: 10.1016/j.future.2016.11.012.
[36] H. D. Kotha and V. M. Gupta, "IoT application: A survey," Int. J. Eng. Technol., vol. 7, no. 2.7, pp. 891–896, 2018.
[37] S. Neelakandan, M. A. Berlin, S. Tripathi, et al., "IoT-based traffic prediction and traffic signal control system for smart city," Soft Comput., vol. 25, pp. 12241–12248, 2021, doi: 10.1007/s00500-021-05896-x.
[38] A. K. Sikder, A. Acar, H. Aksu, A. S. Uluagac, K. Akkaya and M. Conti, "IoT-enabled smart lighting systems for smart cities," 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2018, pp. 639-645, doi: 10.1109/CCWC.2018.8301744.
[39] P. Netinant, T. Utsanok, M. Rukhiran, and S. Klongdee, "Development and assessment of Internet of Things-driven smart home security and automation with voice commands," IoT, vol. 5, no. 1, pp. 79–99, 2024, doi: 10.3390/iot5010005.
[40] A. Alsharif, A. Alzahrani, and B. Alotaibi, "IoT-based smart waste bin monitoring and municipal solid waste management system," Arabian Journal for Science and Engineering, vol. 45, no. 10, pp. 8887–8900, 2020, doi: 10.1007/s13369-020-04637-w.
[41] S. Kaza, L. Yao, P. Bhada-Tata, and F. Van Woerden, What a Waste 2.0: A Global Snapshot of Solid Waste Management to 2050. Washington, DC, USA: World Bank, 2018, doi: 10.1596/978-1-4648-1329-0.
[42] M. R. Alam, M. B. I. Reaz, and M. A. M. Ali, "A review of smart homes—Past, present, and future," IEEE Trans. Syst., Man, Cybern. C (Appl. Rev.), vol. 42, no. 6, pp. 1190–1203, Nov. 2012, doi: 10.1109/TSMCC.2012.2189204.
[43] M. Soori, B. Arezoo, and R. Dastres, "A review of Industry 4.0 and its enabling technologies: IoT, cyber-physical systems, and artificial intelligence," Internet of Things and Cyber-Physical Systems, vol. 3, pp. 1–15, 2023, doi: 10.1016/j.iotcps.2023.04.006.
[44] S. Sinha, "State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally," IoT Analytics, Oct. 2025.
[45] M. Soori, F. K. Ghaleh Jough, R. Dastres, and B. Arezoo, "AI-based decision support systems in Industry 4.0: A review," Journal of Engineering and Emerging Technologies, 2024, doi: 10.1016/j.ject.2024.08.005.
[46] H. Khujamatov, E. Reypnazarov, D. Khasanov, and N. Akhmedov, "IoT, IIoT, and cyber-physical systems integration," in Emergence of Cyber Physical System and IoT in Smart Automation and Robotics, K. K. Singh, A. Nayyar, S. Tanwar, and M. Abouhawwash, Eds. Cham, Switzerland: Springer, 2021, pp. 33–49, doi: 10.1007/978-3-030-66222-6_3.
[47] M. Abd Elghany and N. Elessawi, "The role of Industry 5.0 Internet of Things adoption on sustainable performance of manufacturing SMEs through the integration of supply chain," Discover Computing, vol. 29, Art. no. 28, 2026, doi: 10.1007/s10791-025-09797-7.
[48] S. Al-Sarawi, M. Anbar, R. Abdullah, and A. B. Al Hawari, "Internet of Things market analysis forecasts, 2020–2030," in Proc. 4th World Conf. Smart Trends Syst., Security Sustainability (WorldS4), London, UK, 2020, pp. 449–453, doi: 10.1109/WorldS450073.2020.9210375.
[49] S. K. Sharma, M. S. Raza, and S. A. Alqahtani, "Internet of Things (IoT): Applications, challenges, and future directions," IEEE Access, vol. 12, pp. 12345–12367, 2024, doi: 10.1109/ACCESS.2024.3356789.
[50] C. Conrad, S. Al-Rubaye, and A. Tsourdos, "Intelligent embedded systems platform for vehicular cyber-physical systems," Electronics, vol. 12, no. 13, p. 2908, 2023, doi: 10.3390/electronics12132908.
[51] M. A. Rahman, S. B. Alam, K. D. Gupta, R. George, S. Siddique, and K. Kobayashi, "Understanding communication and protocols in ICS: Securing network infrastructure and data exchange," in Securing Industrial Control Systems. Cham, Switzerland: Springer, 2026, doi: 10.1007/978-3-032-03018-4_3.
[52] A. Yousefpour, G. Ishigaki, and J. P. Jue, "Fog computing: Towards minimizing delay in the Internet of Things," IEEE Commun. Mag., vol. 57, no. 5, pp. 54–61, May 2019, doi: 10.1109/MCOM.2019.1800457.
[53] Y. Lu and X. Xu, "Cloud-based manufacturing equipment and big data analytics to enable on-demand manufacturing services," Robotics and Computer-Integrated Manufacturing, vol. 57, pp. 92–102, 2019, doi: 10.1016/j.rcim.2018.11.006.
[54] X. Xu, Y. Lu, B. Vogel-Heuser, and L. Wang, "Industry 4.0 and Industry 5.0—Inception, conception and perception," Journal of Manufacturing Systems, vol. 61, pp. 530–535, 2021, doi: 10.1016/j.jmsy.2021.10.006.
[55] W. J. Ladeira, W. M. Lim, F. de Oliveira Santini, et al., "Industrial Internet of Things (IIoT)," Electronic Commerce Research, 2026, doi: 10.1007/s10660-026-10097-5.
[56] M. S. Farooq, M. Abdullah, S. Riaz, A. Alvi, F. Rustam, M. A. L. Flores, J. C. Galán, M. A. Samad, and I. Ashraf, "A survey on the role of industrial IoT in manufacturing for implementation of smart industry," Sensors, vol. 23, no. 21, p. 8958, 2023, doi: 10.3390/s23218958.
[57] M. A. D. Martínez, R. V. R. Salinas, R. D. C. V. Castilleja, M. A. M. Rodriguez, G. C. Zubirias, Y. A. F. Rubio, et al., "The impact of the Internet of Things on corporate sustainability in the Industry 4.0 era: A systematic literature review," Results in Engineering, 2026, Art. no. 109304, doi: 10.1016/j.rineng.2026.109304.
[58] S. Afrin, S. J. Rafa, M. Kabir, T. Farah, M. S. B. Alam, A. Lameesa, et al., "Industrial Internet of Things: Implementations, challenges, and potential solutions across various industries," Computers in Industry, vol. 170, p. 104317, 2025, doi: 10.1016/j.compind.2025.104317.
[59] Z. Wu, K. Qiu, and J. Zhang, "A smart microcontroller architecture for the Internet of Things," Sensors, vol. 20, no. 7, p. 1821, 2020, doi: 10.3390/s20071821.

[60] M. Haghi, K. Thurow, and R. Stoll, "Wearable devices in medical Internet of Things: Scientific research and commercially available devices," Healthcare Informatics Res., vol. 23, no. 1, pp. 4–15, 2017, doi: 10.4258/hir.2017.23.1.4.
[61] M. S. Hossain and G. Muhammad, "Healthcare big data voice pathology assessment framework for smart cities," IEEE Access, vol. 7, pp. 178857–178866, 2019, doi: 10.1109/ACCESS.2019.2957124.
[62] A. Al Dakheel, M. Del Pero, R. Aste, and F. Leonforte, "Smart buildings features and key performance indicators: A review," Sustain. Cities Soc., vol. 61, Art. no. 102328, 2020, doi: 10.1016/j.scs.2020.102328.
[63] M. Wei, S. K. Firth, and T. M. Hassan, "Predictive maintenance for building energy systems using IoT and machine learning," Energy Build., vol. 253, Art. no. 111523, 2021, doi: 10.1016/j.enbuild.2021.111523.
[64] J. Zhang, Y. Li, and H. Wang, "IoT-enabled smart buildings for sustainable smart cities: A comprehensive review," Sustain. Cities Soc., vol. 107, Art. no. 105512, 2026, doi: 10.1016/j.scs.2025.105512.
[65] H. Menouar, F. Filali, and M. Lenardi, "A survey and qualitative analysis of recent advances in vehicular networking," IEEE Commun. Surveys Tuts., vol. 23, no. 2, pp. 1016–1051, 2021, doi: 10.1109/COMST.2021.3050818.
[66] D. Oladimeji, K. Gupta, N. A. Kose, K. Gundogan, L. Ge, and F. Liang, "Smart transportation: An overview of technologies and applications," Sensors, vol. 23, no. 8, p. 3880, 2023, doi: 10.3390/s23083880.
[67] Q. Wei, W. Wang, and H. Huang, "Fundamentals for industrial internet security," in Industrial Internet Security. Singapore: Springer, 2025, doi: 10.1007/978-981-96-5135-1_2.
[68] F. Dinmohammadi, A. M. Farook, and M. Shafiee, "Improving energy efficiency in buildings with an IoT-based smart monitoring system," Energies, vol. 18, no. 5, p. 1269, 2025, doi: 10.3390/en18051269.
[69] K. Zhang, Y. Zhu, S. Maharjan, and Y. Zhang, "Edge intelligence and reinforcement learning for resource management in Internet of Things," IEEE Netw., vol. 35, no. 5, pp. 38–45, Sept.–Oct. 2021, doi: 10.1109/MNET.011.2000665.
[70] Y. Liu, J. Ding, and X. Wang, "Reinforcement learning in cyber-physical systems: A survey," IEEE Trans. Neural Netw. Learn. Syst., vol. 33, no. 5, pp. 1659–1677, May 2022, doi: 10.1109/TNNLS.2021.3066588.
[71] A. K. Sangaiah, M. S. Hossain, G. Muhammad, and A. Castiglione, "Internet of Things and big data analytics for smart and connected communities," Future Gener. Comput. Syst., vol. 92, pp. 1051–1054, 2019, doi: 10.1016/j.future.2017.10.021.
[72] S. Mirjalili, S. M. Mirjalili, and A. Lewis, "Grey wolf optimizer," Adv. Eng. Softw., vol. 69, pp. 46–61, 2014, doi: 10.1016/j.advengsoft.2013.12.007.
[73] N. Basil, B. M. Sabbar, H. M. Marhoon, A. F. Mohammed, and A. Ma'arif, "Systematic review of unmanned aerial vehicles control: Challenges, solutions, and meta-heuristic optimization," Int. J. Robot. Control Syst., vol. 4, no. 4, pp. 1794–1818, 2024, doi: 10.31763/ijrcs.v4i4.1596.
[74] H. Zhu, Y. Cao, W. Wang, T. Jiang, and S. Jin, "Deep reinforcement learning for mobile edge computing: A survey," IEEE Commun. Surveys Tuts., vol. 22, no. 4, pp. 2043–2068, 2020, doi: 10.1109/COMST.2020.2987847.
[75] H. M. Marhoon, B. M. Sabbar, N. Qasem, N. Basil, and A. Ma'arif, "Safety and surveillance on unmanned aerial vehicles control systems and optimization methods: A systematic review," Int. J. Robot. Control Syst., vol. 5, no. 5, pp. 2589–2611, 2025, doi: 10.31763/ijrcs.v5i5.1859.
[76] N. Basil, H. M. Marhoon, B. M. Sabbar, et al., "Multi-criteria decision model for multicircular flight control of unmanned aerial vehicles through a hybrid approach," Scientific Reports, vol. 15, Art. no. 18962, 2025, doi: 10.1038/s41598-025-01508-y.
[77] A. Al-Fuqaha, A. Khreishah, M. Guizani, A. Rayes, and M. Mohammadi, "Toward better horizontal integration among IoT services," IEEE Communications Magazine, vol. 53, no. 9, pp. 72–79, Sept. 2015, doi: 10.1109/MCOM.2015.7263379.
[78] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the Internet of Things in the age of machine learning and software-defined networking," IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4829–4842, Dec. 2018, doi: 10.1109/JIOT.2018.2846040.
[79] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, M. Imran, and M. Guizani, "Internet of Things architecture: Recent advances, taxonomy, requirements, and open challenges," IEEE Wireless Communications, vol. 24, no. 3, pp. 10–16, June 2017, doi: 10.1109/MWC.2017.1600421.
[80] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," Journal of Information Security and Applications, vol. 50, p. 102419, 2020, doi: 10.1016/j.jisa.2019.102419.
[81] T. N. Gia, M. Jiang, A. M. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen, "Fog computing in healthcare Internet of Things: A case study on ECG feature extraction," IEEE Access, vol. 7, pp. 1353–1363, 2019, doi: 10.1109/ACCESS.2018.2885480.
[82] M. Bennis, M. Debbah, and H. V. Poor, "Ultra-reliable and low-latency wireless communication: Tail, risk, and scale," Proceedings of the IEEE, vol. 106, no. 10, pp. 1834–1853, Oct. 2018, doi: 10.1109/JPROC.2018.2867029.
[83] J. Konečný, H. B. McMahan, D. Ramage, and P. Richtárik, "Federated optimization: Distributed machine learning for on-device intelligence," IEEE Signal Processing Magazine, vol. 38, no. 3, pp. 50–60, May 2021, doi: 10.1109/MSP.2020.3049903.
[84] P. Warden and D. Situnayake, "TinyML: Machine learning with TensorFlow Lite on Arduino and ultra-low-power microcontrollers," O'Reilly Media, 2019.
[85] Q. Qi and F. Tao, "Digital twin and big data towards smart manufacturing and Industry 4.0: 360 degree comparison," IEEE Access, vol. 6, pp. 3585–3593, 2018, doi: 10.1109/ACCESS.2018.2793265.
[86] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.
[87] J. Garcıa and F. Fernández, "A comprehensive survey on safe reinforcement learning," Journal of Machine Learning Research, vol. 16, pp. 1437–1480, 2015.
[88] S. Ahmad, M. S. Farooq, and T. A. Alghamdi, "Deep learning models for cloud, edge, fog, and IoT: A survey," J. Netw. Comput. Appl., vol. 205, Art. no. 103452, 2023, doi: 10.1016/j.jnca.2022.103452.
[89] A. Maghsoudnia, S. Banerjee, A. Dutta, and A. Schulman, "Ultra-reliable low-latency in 5G: A close reality or a distant dream?," in Proc. ACM HotNets, 2024, pp. 1–7, doi: 10.1145/3696347.3696375.
[90] M. H. Alsharif, A. Kelechi, and R. Nordin, "A contemporary survey of recent advances in federated learning: Taxonomies, applications, and challenges," ICT Express, vol. 10, no. 4, pp. 798–823, 2024, doi: 10.1016/j.icte.2023.11.003.
[91] J. P. A. Yaacoub, H. N. Noura, and O. Salman, "Security of federated learning with IoT systems: Issues, challenges, and future directions," Digit. Commun. Netw., vol. 9, no. 2, pp. 277–295, 2023, doi: 10.1016/j.dcan.2022.02.003.
[92] S. Silvestri, D. Monaco, A. Sacco, and G. Marchetto, "A review on the emerging technology of TinyML," ACM Comput. Surveys, vol. 56, no. 10, Art. no. 230, 2024, doi: 10.1145/3649398.

ISSN:2222-758X
e-ISSN:2789-7362

[93] S. Heydari, M. B. Shokrollahi, and A. H. Jahangir, "Tiny machine learning and on-device inference: A survey," Sensors, vol. 25, no. 10, Art. no. 3191, 2025, doi: 10.3390/s25103191.
[94] A. A. A. Ardebili, M. Zappatore, A. I. H. A. Ramadan, A. Longo, and A. Ficarella, "Digital twins of smart energy systems: A systematic literature review," Energy Informatics, vol. 7, Art. no. 94, 2024, doi: 10.1186/s42162-024-00319-7.
[95] S. Djebali, S. Mosbah, and N. Tabbane, "Survey and insights on digital twins design and smart grid's potential," Future Gener. Comput. Syst., vol. 151, pp. 600–621, 2024, doi: 10.1016/j.future.2023.10.019.
[96] M. A. Azad, M. F. Z. Ayob, M. H. A. Hijazi, and J. Han, "Verify and trust: A multidimensional survey of zero-trust," J. Ind. Inf. Integr., vol. 35, Art. no. 100544, 2024, doi: 10.1016/j.jii.2023.100544.
[97] S. H. Gopalan, S. G. Ramasamy, and M. Natarajan, "Enhancing IoT security: A blockchain-based mitigation of deauthentication attacks," Blockchain: Res. Appl., vol. 3, Art. no. 100047, 2024, doi: 10.1016/j.bcra.2022.100047.
[98] E. Hedrick, B. N. Nguyen, and F. Boukouvala, "Reinforcement learning for online adaptation of model predictive controllers," Comput. Chem. Eng., vol. 160, Art. no. 107728, 2022, doi: 10.1016/j.compchemeng.2022.107728.
[99] D. Sun, C. Chen, and Y. Li, "Adaptive parameterized model predictive control based on reinforcement learning," Expert Syst. Appl., vol. 244, Art. no. 122983, 2024, doi: 10.1016/j.eswa.2023.122983.
[100] D. R. Han, X. Yuan, and W. Yin, "A survey on some recent developments of alternating direction method of multipliers," J. Oper. Res. Soc. China, vol. 10, pp. 283–307, 2022, doi: 10.1007/s40305-021-00351-4.
[101] K. Xu, G. Chen, and Q. Jiang, "A distributed consensus-based algorithm for economic dispatch in smart grids," IET Control Theory Appl., vol. 17, no. 7, pp. 1083–1094, 2023, doi: 10.1049/cth2.12438.
[102] M. A. Khan, M. T. Quasim, N. Javaid, M. A. Khan, and M. Ilahi, "A comprehensive survey on smart cities: IoT applications, architectures, and future trends," Sustainable Cities and Society, vol. 61, Art. no. 102292, 2020, doi: 10.1016/j.scs.2020.102292.
[103] Statista, "Smart home—Worldwide market forecast 2023–2025," 2024. Available: https://www.statista.com/outlook/dmo/smart-home/worldwide.
[104] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for IoT big data and streaming analytics: A survey," IEEE Communications Surveys Tutorials, vol. 20, no. 4, pp. 2923–2960, 2018, doi: 10.1109/COMST.2018.2844341.
[105] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, "Federated optimization in heterogeneous networks," Proceedings of Machine Learning and Systems, vol. 2, pp. 429–450, 2020.
[106] Y. Ren, Z. Wang, P. K. Sharma, F. Alqahtani, A. Tolba, and J. Wang, "Zero trust networks: Evolution and application from concept to practice," Computers, Materials Continua, 2025, doi: 10.32604/cmc.2025.059170.
[107] M. M. Salim, M. Kim, S. K. Singh, and J. H. Park, "Zero-trust blockchain-enabled framework for scalable and secure IoT networks," Future Gener. Comput. Syst., vol. 175, p. 108093, 2026, doi: 10.1016/j.future.2025.108093.
[108] S. S. Gill, M. Xu, I. Singh, K. K. Chahal, and S. Kaur, "Transformative effects of IoT, blockchain and artificial intelligence on cloud computing: Evolution, vision, trends and open challenges," Internet of Things, vol. 8, Art. no. 100118, 2019, doi: 10.1016/j.iot.2019.100118.
[109] A. Holzinger, G. Langs, H. Denk, K. Zatloukal, and H. Müller, "Causability and explainability of artificial intelligence in medicine," Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, vol. 9, no. 4, Art. no. e1312, 2019, doi: 10.1002/widm.1312.
[110] S. Faye, R. Decorme, et al., "A reference functional architecture for network digital twins in 6G systems," IEEE Open Journal of the Communications Society, 2026, doi: 10.1109/OJCOMS.2026.3668035.