A Survey of Services Exploding AI Internet of Things Internet of People Internet of Thinking Artificial General Intelligence Cyber-Physical Systems and Smart Environments

Abstract

The rapid evolution of interconnected technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), Cyber-Physical Systems (CPS), and smart environments is transforming human-computer interactions and automating complex processes across diverse sectors. This survey explores the convergence of these technologies, highlighting their role in creating adaptive and responsive environments that enhance operational efficiency and societal well-being. It examines the integration of AI into IoT frameworks, emphasizing the significance of ubiquitous connectivity and seamless interaction between the physical and digital worlds. The survey also addresses the challenges of interoperability, security, and privacy, which are critical in managing the complexities of these interconnected systems. It underscores the need for robust frameworks and interdisciplinary collaboration to develop comprehensive security measures and ensure the safe deployment of these technologies. Furthermore, the survey identifies future research directions, including the enhancement of interoperability, the development of scalable security solutions, and the exploration of ethical and societal implications. By fostering innovation and responsible practices, these technologies can significantly contribute to economic growth and societal advancement. The survey concludes by emphasizing the importance of ongoing research and development to address existing challenges and harness the opportunities presented by these transformative technologies.

1 Introduction

1.1 Technological Landscape Overview

The contemporary technological landscape is significantly influenced by the convergence of advanced technologies, including Artificial Intelligence (AI), the Internet of Things (IoT), the Internet of People (IoP), Artificial General Intelligence (AGI), Cyber-Physical Systems (CPS), and smart environments. This integration fosters seamless interactions between physical and digital realms, creating adaptive environments across diverse applications such as healthcare, education, smart cities, and entertainment. High-speed data communications, mobile edge computing, and digital twins enhance user engagement and satisfaction by addressing interactivity and authenticity requirements [1, 2, 3, 4]. The incorporation of AI into IoT amplifies capabilities within smart environments, enriching user experiences across various sectors.

The IoT extends device interconnectivity beyond traditional computing systems, facilitating transformative impacts across industries [5]. The edge-cloud continuum (ECC) exemplifies this integration, highlighting the synergy between IoT and cloud computing [6]. Autonomy is a key concept within

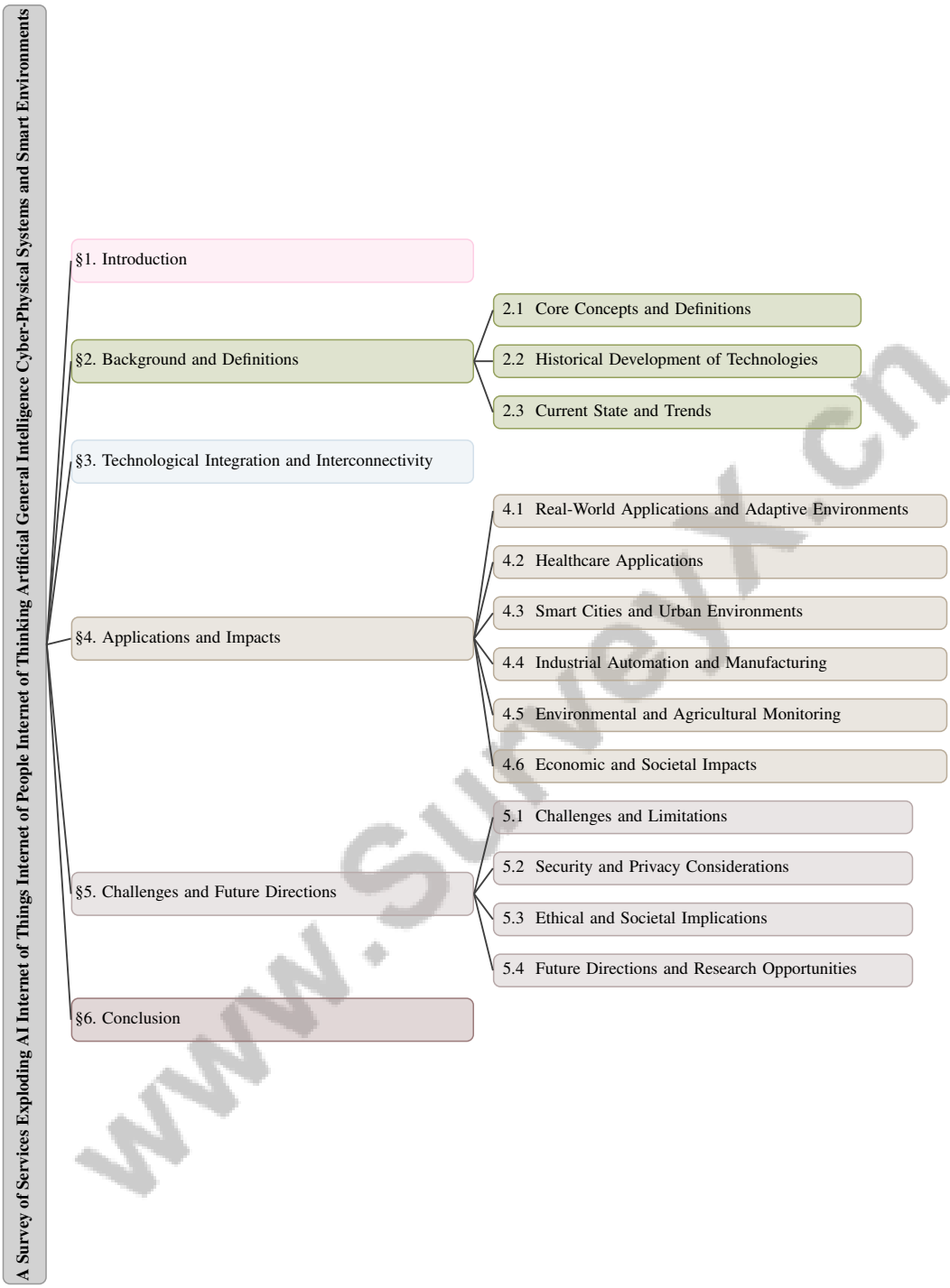


Figure 1: chapter structure

IoT, promising smart services and systems that achieve global objectives such as optimal resource management with minimal human intervention [7].

The IoP adds a human-centric dimension, emphasizing the role of users in the data-centric Internet, driven by the proliferation of personal mobile and IoT devices [8]. The emergence of Cyber-Physical Social Machines (CPSMs) illustrates the dynamic nature of these interconnected systems [9].

Advancements in AI and robotics necessitate improved human-robot collaboration methods, addressing limitations of existing remote control technologies [10]. The potential risks associated with rapid

AI advancements, particularly with generalist AI systems capable of autonomous action, are critical considerations in this landscape [11].

Self-adaptive architectures in IoT systems address the challenges of dynamic environmental changes affecting Quality of Service (QoS) [6]. The Internet of Federated Things (IoFT) emphasizes decentralized, privacy-preserving model training in IoT systems, underscoring the importance of security and privacy [5].

The convergence of machine learning, IoT, and robotics is revolutionizing smart environments, enhancing functionality and adaptability. This convergence drives innovation while presenting challenges and opportunities for research and development. As smart infrastructures like Smart Cities, Smart Grids, and Smart Health systems evolve, they demand robust wireless connectivity and dynamic integration of IoT devices, which now outnumber traditional internet-connected devices. Current trends indicate that while information services technologies are reaching saturation, sectors like smart homes/buildings and smart grids are in development, necessitating ongoing investment and exploration to meet emerging needs in agility, reliability, and scalability. The ongoing evolution of these interconnected technologies underscores the need for effective technology forecasting and innovative solutions, such as context-aware dynamic discovery systems, to optimize resource management and decision-making in increasingly complex environments [12, 13, 3].

1.2 Significance of AI and IoT

The convergence of Artificial Intelligence (AI) and the Internet of Things (IoT) is crucial for technological advancement, significantly transforming various sectors. This integration enhances operational efficiencies and addresses challenges such as high latency, bandwidth consumption, and privacy issues inherent in traditional cloud computing methods [5]. Deploying Convolutional Neural Networks (CNNs) on resource-constrained IoT devices exemplifies edge intelligence's potential to facilitate real-time processing and decision-making.

In manufacturing, the transition to Smart Factories through IoT integration addresses knowledge gaps in enhancing processes, driving the evolution of Industry 4.0 [14]. The transformation of traditional factories into intelligent systems underscores IoT's role in optimizing production efficiency and data-driven decision-making. Additionally, the expansion of online advertising into the IoT domain presents a promising yet under-explored research avenue, leveraging the vast data generated by IoT devices to innovate advertising strategies.

The IoP introduces a human-centric approach to data management, where personal devices serve as proxies for users, enhancing user-centric data interactions. This shift fosters meaningful human-machine interactions and enriches the user experience [15].

In healthcare, AI and IoT integration significantly benefits chronic condition management and supports the aging population. Technology-based solutions, such as augmented personalized health (APH), leverage AI and IoT to improve health outcomes by utilizing diverse data sources [16]. However, the potential for large-scale social harms and malicious uses of AI necessitates careful examination of its societal implications [17].

Despite advancements, challenges persist in integrating AI and IoT, particularly concerning the complexities of human-machine interactions and associated privacy and security implications. The security risks posed by generative AI in IoT systems require urgent attention to identify and mitigate vulnerabilities [18]. Furthermore, enhancing human-AI interactions can help mitigate risks of homogenization and bias, emphasizing the need for a balanced approach to AI deployment [19].

Collectively, the integration of AI and IoT is pivotal in shaping the future of technology, presenting significant opportunities and challenges across sectors. As these technologies evolve, they will play a critical role in developing adaptive environments, fostering human-AI coevolution, and driving technological innovation [20].

1.3 Structure of the Survey

This survey is meticulously structured to provide a comprehensive exploration of the interconnected technologies shaping the modern digital landscape. It begins with an **Introduction** that sets the stage by examining the technological landscape characterized by the convergence of AI, IoT, IoP,

AGI, CPS, and smart environments, highlighting their significance in enhancing human-computer interactions and automating complex processes.

Following the introduction, the survey delves into the **Background and Definitions**, offering detailed explanations of core concepts such as AI, IoT, IoP, AGI, CPS, and smart environments. This section covers the historical development and current state of these technologies, providing context for understanding their evolution and trends.

The next section, **Technological Integration and Interconnectivity**, explores how these technologies interact to create adaptive environments. It discusses the role of ubiquitous connectivity and seamless integration between physical and digital worlds, examining frameworks and models that facilitate this integration while addressing interoperability and data management challenges.

In **Applications and Impacts**, the survey evaluates the practical applications of these technologies across domains such as healthcare, smart cities, and industrial automation, highlighting their transformative potential and broader economic and societal impacts.

The penultimate section, **Challenges and Future Directions**, identifies key challenges in implementing and developing these technologies, including security, privacy, and ethical considerations. It proposes potential future research directions and opportunities to overcome these challenges, emphasizing the need for continued innovation and adaptation.

The **Conclusion** synthesizes the survey's principal findings, emphasizing the implications of the evolving technological landscape—particularly the interplay between regulatory frameworks, market dynamics, and emerging technologies like 5G and AI—on future research and development in internet services and IoT. It underscores the necessity for comprehensive regulatory policies to foster innovation and investment while addressing risks associated with technological hype, particularly in AI, advocating for a balanced approach to mitigate these risks in future advancements [21, 22, 3]. This structured approach ensures a comprehensive understanding of the complex interplay between these technologies and their societal impacts.The following sections are organized as shown in Figure 1.

2 Background and Definitions

2.1 Core Concepts and Definitions

The technological landscape is driven by core concepts such as Artificial Intelligence (AI), the Internet of Things (IoT), the Internet of People (IoP), and Cyber-Physical Systems (CPS), each contributing to innovation across sectors. AI, encompassing machine learning and natural language processing, enhances systems' capabilities, particularly when integrated into 5G networks, addressing data rate and latency challenges [23]. The pursuit of Artificial General Intelligence (AGI) raises both prospects and ethical concerns, with risks associated with misaligned superhuman AGI [24, 19].

IoT, characterized by autonomous device communication, impacts healthcare, transportation, and industry, but faces challenges in connectivity and security [14, 25]. Effective IoT deployment requires addressing interoperability issues and ensuring security distinct from traditional IT systems [26, 27]. IoP emphasizes human-centric data management and interactions, enhancing user engagement through personal devices [28].

CPS integrate computation with physical processes, enabling real-time interactions essential for smart environments. Fog and Edge Computing extend capabilities to the network's edge, meeting demands for agility and security [27]. Smart environments, leveraging AI, enhance efficiency in applications like smart cities and healthcare, where integrated systems address chronic disorder management [19]. These technologies, including Digital Twins and Edge Intelligence, drive innovation in sectors such as agriculture by improving interoperability and decision-making [29].

The foundational concepts of AI, IoT, IoP, and CPS underscore the interconnected technological landscape, fostering innovation through enhanced connectivity and intelligent systems. Ethical and socio-cultural considerations are vital as these technologies evolve [30].

2.2 Historical Development of Technologies

Technological evolution in AI, IoT, CPS, and smart environments has been marked by significant milestones. IoT's progression from basic networking to sophisticated systems has facilitated smart

community development, necessitating decentralized approaches to manage dynamic environments [28, 9]. IoP's integration of human behavior models enhances digital interactions, emphasizing the importance of human dynamics in system design [31, 32, 33].

CPS advancements, exemplified by the 5C architecture, enable seamless integration of computational and physical processes, enhancing adaptability [34]. Self-adaptive IoT architectures address dynamic events through integrated adaptation strategies [35]. The development of smart environments, including digital twins, has been facilitated by ontologies that enhance knowledge representation [36].

In intelligent manufacturing, optimizing cloud service composition is crucial for effective service configuration [37]. The rise of social machines, influenced by IoT, highlights IoT's role in shaping digital ecosystems [18]. The historical trajectory of these technologies emphasizes overcoming integration and resource management challenges, focusing on scalability and seamless interaction between physical and digital realms [25].

2.3 Current State and Trends

The current technological landscape is defined by the rapid integration of AI, IoT, CPS, and smart environments, driven by the need for interoperability, efficiency, and security. AI's integration with IoT and CPS enhances predictive analytics and operational efficiency, particularly in industrial applications [24]. However, accessibility issues for non-technical users and limited safety research pose risks [20, 38].

IoT's complexity and device heterogeneity challenge integration and data management, necessitating gateways for protocol interoperability [25, 26]. CPS advancements focus on self-adaptive architectures to enhance QoS, while IoFT introduces challenges in achieving seamless integration in decentralized environments [35, 39].

Smart environments face challenges in heterogeneity and data incompatibility, impacting multi-hazard system development [40]. Innovations in edge intelligence improve throughput and reduce latency, addressing edge-cloud environment challenges [41]. Security risks encompass privacy, model security, and malicious AI use, highlighting the need for robust frameworks [42, 7].

The current state and trends underscore the necessity for robust platforms to overcome challenges, facilitating the sustained evolution of AI, IoT, CPS, and smart environments. Addressing interoperability, security, and resource management is essential to fully harness these transformative technologies [43].

3 Technological Integration and Interconnectivity

Category	Feature	Method
Interconnectivity and Integration	Adaptive Systems Human-Focused Models	IPAF[14], DPM[44], MHEWS[40] SM[19]
Interoperability and Data Management	Protocol Handling	GIoT-M[26]

Table 1: This table provides a comprehensive summary of methods categorized under interconnectivity and integration, and interoperability and data management within IoT, AI, and CPS technologies. It highlights specific features such as adaptive systems and protocol handling, alongside the associated methodologies, emphasizing their roles in enhancing operational efficiency and data management.

The integration of digital systems is pivotal for enhancing operational efficiencies and responsiveness across various sectors. Table 1 presents a detailed summary of methodologies relevant to interconnectivity, integration, and data management, highlighting the importance of these technologies in achieving seamless integration and operational efficiency. Table 2 offers a comprehensive comparison of different methodologies pertinent to technological integration, emphasizing their roles in achieving seamless interconnectivity and efficient data management. This section explores the interplay between technological integration and interconnectivity, emphasizing the role of emerging technologies in facilitating seamless interactions between physical and digital realms.

3.1 Interconnectivity and Integration

The convergence of the Internet of Things (IoT), Artificial Intelligence (AI), and Cyber-Physical Systems (CPS) is crucial for achieving ubiquitous connectivity and seamless integration. This integration fosters adaptive environments that enhance operational efficiency. The IoT Process Awareness Framework (IPAF) exemplifies this by systematically extracting and correlating process-related information from IoT data, enabling informed decision-making [14]. AI's integration into 5G networks is vital for resource management and network security, illustrating the convergence of digital and physical communication systems [23]. Interoperability challenges within IoT are categorized into technical, semantic, syntactic, and cross-domain aspects, which are essential for effective integration [25].

Middleware technologies facilitate efficient data management and application integration within IoT platforms. Microservice-based middleware enhances interoperability and data integration, crucial for applications like Early Warning Systems (EWS), where timely data exchange is essential [40]. In industrial contexts, dynamic adaptation and reconfiguration optimize resource utilization and improve system responsiveness. The dynamic partitioning methodology (DPM) demonstrates this by distributing Convolutional Neural Network (CNN) layers across resource-constrained devices, achieving faster and more accurate inference [44]. This highlights the significance of adaptive AI systems that adjust dynamically based on various parameters.

The Internet of People (IoP) introduces a human-centric perspective, treating personal devices as active network nodes capable of self-organization. This shift to a human-centric data management model incorporates human behavior into algorithms, enhancing digital interconnectedness [31]. The SocialMuse method exemplifies this by utilizing predictive models to recommend peers, fostering an interconnected environment that enhances creativity [19].

Security remains a critical concern in increasingly interconnected environments, as the proliferation of IoT technologies introduces vulnerabilities and potential attack vectors. Establishing robust frameworks that ensure secure connectivity and uphold data integrity is essential. This requires an interdisciplinary approach involving cybersecurity experts, network architects, and system designers to develop solutions that defend against both known and emerging threats, fostering a secure IoT ecosystem that supports global economic growth and technological advancement [45, 21, 46]. Decentralized networks facilitate secure communications among IoT devices, crucial for sensitive applications, while layered security protocols in IoT analytics address environment-specific vulnerabilities.

The integration of IoT, AI, and CPS promotes ubiquitous connectivity, bridging physical and digital realms to create adaptive environments responsive to user needs. This interconnectedness is vital for driving technological innovation and addressing the complexities of managing dynamic systems, particularly in the context of Industry 4.0 and 5.0, which aim to develop smarter, more sustainable solutions and enhance infrastructure resilience [47, 21, 3].

As illustrated in Figure 2, the key components and methodologies involved in achieving interconnectivity and integration within the realms of IoT, AI, and CPS are highlighted. This figure emphasizes the convergence of technologies, middleware solutions, and human-centric models as pivotal elements driving operational efficiency, adaptive environments, and enhanced security. Frameworks and architectures that support seamless integration and interoperability are crucial for realizing the potential of these transformative technologies.

3.2 Layered Frameworks and Architectural Models

Layered frameworks and architectural models are crucial in integrating AI and IoT, addressing the complexities of these technologies to achieve seamless interoperability and efficient data management. One approach categorizes the IoT landscape into distinct layers—application, data abstraction, data accumulation, edge computing, connectivity, and edge devices—each critical for ensuring effective communication within IoT systems [48].

In mobile ultra-broadband, THz communications aim for high data rates, complemented by the concept of super IoT, which employs symbiotic radio and satellite-assisted communications to enhance connectivity [49]. The integration of advanced communication technologies into IoT frameworks is essential for supporting modern applications' massive data throughput and low-latency requirements.

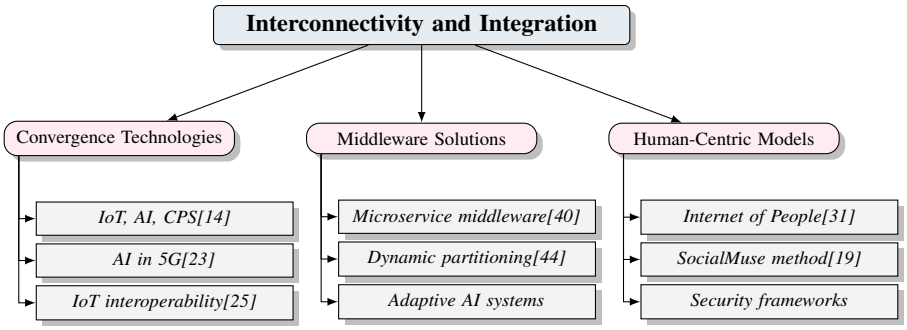
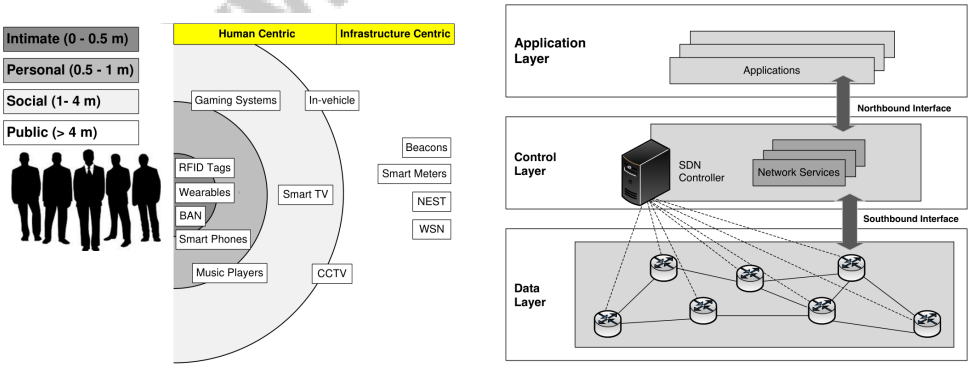


Figure 2: This figure illustrates the key components and methodologies involved in achieving interconnectivity and integration within the realms of IoT, AI, and CPS. It highlights the convergence of technologies, middleware solutions, and human-centric models as pivotal elements driving operational efficiency, adaptive environments, and enhanced security.

Architectural models from massively multiplayer online worlds (MMOWs) provide insights into scalability strategies applicable to IoT environments, emphasizing the management of large-scale, dynamic interactions [50]. By leveraging these strategies, IoT frameworks can better accommodate the growing number of connected devices and the data they generate.

Moreover, integrating AI into these layered frameworks enhances IoT systems' data processing and analysis capabilities, enabling intelligent responses to environmental changes. Deploying AI-driven analytics closer to data sources is crucial for real-time decision-making, significantly reducing latency, particularly for applications such as immersive video conferencing, autonomous vehicles, and emergency response systems [51, 52, 53, 54, 55].

The continuous development of layered frameworks and architectural models is vital for effectively integrating AI and IoT technologies, particularly for real-time applications. This integration is increasingly important as advancements in AI, machine learning, and communication technologies like 5G enable more efficient edge computing solutions, allowing distributed processing closer to data sources. Establishing interoperability among diverse AI and IoT platforms facilitates seamless resource sharing and service composition, ultimately improving system performance and expanding the capabilities of pervasive AI applications across sectors such as healthcare, education, and disaster response [56, 51, 52, 57, 54]. These frameworks enhance IoT systems' overall efficiency and responsiveness, paving the way for advanced, intelligent applications across various domains.



(a) The image depicts a diagram illustrating the relationship between human-centric and infrastructure-centric technologies.[58]

(b) SDN Controller Architecture[59]

Figure 3: Examples of Layered Frameworks and Architectural Models

As illustrated in Figure 3, the exploration of "Technological Integration and Interconnectivity; Layered Frameworks and Architectural Models" presents two examples that delve into the complexities of modern technological ecosystems. The first example is a diagram delineating the relationship between

AI-generated, for reference only.

human-centric and infrastructure-centric technologies, categorized into Intimate, Personal, and Social zones, emphasizing varying proximities and interactions with technology. The second example showcases an SDN (Software-Defined Networking) Controller Architecture, highlighting a layered approach where the SDN controller operates between the data layer and control layer, facilitating seamless communication and management of network services through northbound and southbound interfaces. Together, these examples illustrate how layered frameworks and architectural models bridge human interactions with robust technological infrastructures [58, 59].

3.3 Interoperability and Data Management

The rapid growth of connected devices in the IoT landscape presents significant challenges in achieving interoperability and effective data management. As device numbers increase, managing diverse communication protocols and ensuring seamless data exchange across heterogeneous systems becomes increasingly complex. The demand for high data rates and low latency for real-time applications exacerbates these challenges, necessitating robust solutions for efficient and secure operations in interconnected environments [12].

One effective approach to enhancing interoperability is the GIoT-M method, which improves the handling of multiple communication protocols such as WiFi, Bluetooth, and ZigBee. By transforming data into a uniform format, GIoT-M facilitates seamless integration and communication among devices operating on different protocols, addressing a critical barrier to effective IoT deployment [26]. This method underscores the need for adaptable frameworks capable of managing diverse protocol requirements inherent in IoT systems.

Effective data management in IoT environments requires comprehensive strategies encompassing data collection, storage, analysis, and addressing challenges posed by the vast scale, volume, and variability of sensor-generated data. Real-time analytics and historical trend analysis are crucial for deriving actionable insights [60, 61]. Integrating edge computing with AI-driven analytics at the network's edge is vital for processing data closer to its source, reducing latency, and enhancing real-time decision-making capabilities, thereby improving IoT systems' responsiveness and alleviating the burden on centralized cloud infrastructures.

Managing interconnected IoT devices raises critical security and privacy challenges, as their proliferation across domains such as smart homes and healthcare exposes them to various vulnerabilities and cyber threats. Addressing these concerns necessitates a multifaceted approach combining robust security measures, effective management protocols, and interdisciplinary collaboration among cybersecurity experts, network architects, and system designers to ensure the integrity, confidentiality, and availability of connected systems [45, 62, 63, 64, 25]. Ensuring data integrity and protecting sensitive information from unauthorized access are essential for maintaining trust in IoT systems. Implementing layered security protocols and decentralized network architectures can mitigate potential vulnerabilities, providing a secure foundation for data management in complex IoT environments.

To address interoperability and data management challenges in IoT systems, a comprehensive strategy is essential. This strategy should integrate advanced communication technologies, enable real-time data processing to manage the vast and dynamic data generated by connected devices, and implement stringent security measures to protect against vulnerabilities. Tackling these interconnected issues is crucial for the successful deployment and adoption of IoT applications across various domains [60, 25]. These solutions are vital for unlocking the full potential of IoT technologies and fostering the development of intelligent and adaptive environments.

Feature	Interconnectivity and Integration	Layered Frameworks and Architectural Models	Interoperability and Data Management
Integration Focus	Iot, Ai, Cps	Ai, Iot	Iot Protocols
Technological Components	Middleware, Microservices	Layered Frameworks	Giot-M Method
Security Approach	Interdisciplinary Frameworks	Not Specified	Layered Security Protocols

Table 2: This table provides a comparative analysis of various technological methods focusing on interconnectivity and integration, layered frameworks and architectural models, and interoperability and data management. It highlights key features such as integration focus, technological components, and security approaches, elucidating the diverse strategies employed to enhance operational efficiency and secure data exchange in interconnected environments.

4 Applications and Impacts

The integration of advanced technologies, particularly IoT and AI, has transformative implications across multiple sectors. This section explores the convergence of these technologies, highlighting their impacts on urban living, industrial processes, healthcare, and beyond. As illustrated in Figure 4, the diverse applications and impacts of IoT and AI integration span various sectors. The figure highlights real-world applications that foster adaptive environments, drive healthcare transformations, promote smart city developments, advance industrial automation, and improve environmental monitoring. Furthermore, it underscores the economic and societal implications of these technologies, emphasizing both growth opportunities and ethical considerations that arise from their implementation.

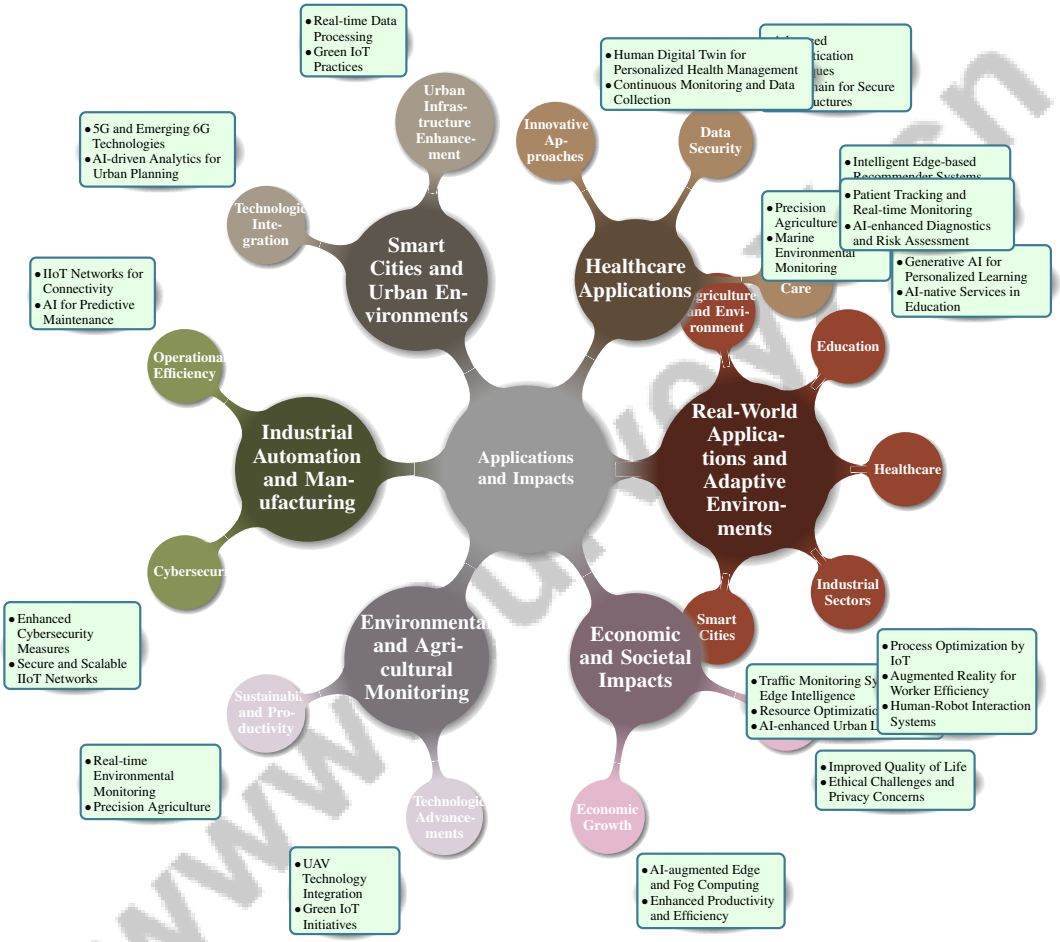


Figure 4: This figure illustrates the diverse applications and impacts of IoT and AI integration across various sectors. It highlights real-world applications fostering adaptive environments, healthcare transformations, smart city developments, industrial automation advancements, and environmental monitoring improvements. Additionally, it underscores the economic and societal implications of these technologies, emphasizing both growth opportunities and ethical considerations.

4.1 Real-World Applications and Adaptive Environments

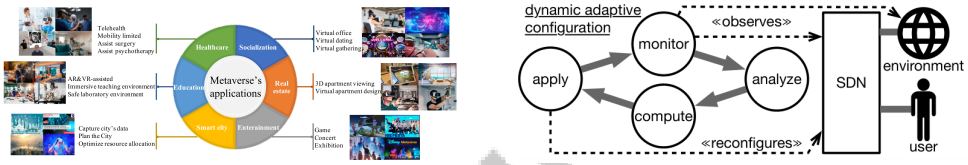
IoT and AI convergence fosters adaptive environments across diverse domains. In smart cities, machine learning enhances urban living through improved traffic management and resource optimization, exemplified by Traffic Monitoring Systems utilizing Edge Intelligence for real-time data analytics [9]. In industrial sectors, IoT optimizes processes, as seen in companies like Siemens AG and General Electric, and enhances worker efficiency through Augmented Reality applications [34]. The Avatar system exemplifies low-latency human-robot interactions, improving operational efficiency and safety [43].

Healthcare benefits from AI and IoT integration through intelligent edge-based recommender systems that promote energy-saving behaviors [65]. AutoML techniques enhance IoT anomaly detection, improving security and operational efficiency [66]. Applications like MoSHub optimize sensor data transmission to the cloud [67].

In education, Generative AI provides personalized learning experiences, creating adaptive environments for student needs [1]. AI-native services, such as writing assistants, demonstrate practical applications in education [20].

The Internet of Behavior influences user behavior towards energy savings, utilizing explainable AI for actionable insights [68]. In agriculture, the Web of Things enhances precision agriculture through improved monitoring and data analysis [69]. IoT-based marine environmental monitoring illustrates digital representation construction in adaptive environments [8].

Systems like mySafeHome dynamically adjust internet access for children based on family presence [70]. The CADDOT model improves sensor discovery and configuration, simplifying IoT adoption for non-technical users [71]. These applications underscore IoT and AI's transformative potential in creating adaptive environments that meet evolving user and industry needs. Proposed frameworks enhance network performance and adaptability [72]. Service mining frameworks and bi-objective optimization methods showcase practical applications in various IoT environments, emphasizing adaptability and performance [41]. An IoT advertising platform acts as an intermediary between advertisers and users, utilizing smart device data to deliver personalized advertisements [73]. Dynamic IoT choreographies enable seamless reconfiguration and failure recovery without centralized control, enhancing reliability and user experience [7].



(a) Metaverse's Applications: A Comprehensive Overview[2]

(b) Dynamic Adaptive Configuration in SDN[74]

Figure 5: Examples of Real-World Applications and Adaptive Environments

As shown in Figure 5, adaptive environments span sectors like the Metaverse and SDN. The Metaverse's integration into various domains highlights its potential to revolutionize interactions and infrastructures. SDN's dynamic adaptive configuration underscores adaptability's significance in modern networking [2, 74].

4.2 Healthcare Applications

IoT and AI integration in healthcare transforms patient care, resource management, and health outcomes. IoT applications like patient tracking and real-time monitoring enhance healthcare quality [15]. IoT devices facilitate seamless data exchange, improving service delivery efficiency.

AI enhances diagnostics, risk assessment, and public health planning by analyzing complex medical data. Incorporating AI into healthcare governance frameworks ensures service safety and efficacy [16]. Generative AI applications in healthcare, including health monitoring and diagnosis, demonstrate these technologies' transformative potential in improving patient care and operational efficiency.

Robust security mechanisms are essential for protecting sensitive patient data, ensuring privacy, and fostering trust in IoT healthcare applications. As IoT devices face increasing vulnerabilities, advanced authentication techniques based on machine learning are necessary to safeguard healthcare systems. Integrating networking and virtualization technologies, such as Blockchain, is crucial for creating secure infrastructures [75, 76]. Efficient resource allocation enhances user satisfaction and health outcomes, emphasizing effective resource management's importance in adaptive environments.

The synergy of IoT and AI in healthcare addresses critical challenges like data security and resource management, advancing personalized medicine. IoT devices enable continuous monitoring and data collection, while AI enhances health data interpretation through machine learning techniques.

This integration meets the demand for timely healthcare services, especially during the COVID-19 pandemic, and fosters trust through robust security measures. Concepts like the Human Digital Twin offer innovative approaches to personalized health management, simulating real-time outcomes and guiding treatment strategies [76, 77]. These advancements pave the way for more adaptive healthcare environments, improving health outcomes and patient satisfaction.

4.3 Smart Cities and Urban Environments

Smart city development is profoundly influenced by integrating IoT, AI, and next-generation communication networks. These technologies enhance urban infrastructure through real-time data processing and resource management, improving mobility via innovative solutions. Green IoT practices aim to minimize environmental impacts, promoting energy efficiency and reducing carbon footprints, aligning with regulatory frameworks and SDGs [12, 78].

Microservices deployment in edge computing optimizes smart city applications. Studies demonstrate microservices enhance deployment and management of smart city infrastructures [79]. AI transforms transportation systems and urban planning, optimizing networks and enhancing public transit efficiency [80]. AI-driven analytics empower city planners to make data-informed decisions, improving urban life quality and contributing to sustainable development.

5G and emerging 6G technologies enhance smart city capabilities, supporting mMTC and URLLC. The IHRA scheme impacts industrial automation and smart city applications by improving communication efficiency [81]. Advanced technologies like machine learning, IoT, and robotics transform urban environments into smart cities, improving resource utilization and connectivity while promoting sustainability. Real-time data from diverse sensors optimize decision-making and enhance public services, fostering cross-sector collaboration. Robust internet service infrastructures support these advancements, achieving SDGs and paving the way for greener, resilient urban living [12, 82].

4.4 Industrial Automation and Manufacturing

IoT integration in industrial automation and manufacturing enhances operational efficiency, flexibility, and scalability. IIoT networks connect machines, systems, and people, providing a robust framework for industrial environments. Martin's reference architecture emphasizes a holistic approach to designing IIoT networks, optimizing manufacturing processes through seamless communication and data exchange [59].

Increased connectivity necessitates a focus on cybersecurity. Blowers underscores the need for enhanced cybersecurity measures to protect industrial environments from threats [83]. AI automates industrial processes in predictive maintenance, quality control, and supply chain optimization. AI-driven analytics enable manufacturers to anticipate equipment failures, optimize production schedules, and enhance efficiency [80].

Advancements in cloud service composition optimize manufacturing processes. Li highlights progress in defining optimization objectives and developing algorithms that enhance service quality and efficiency [37]. These advancements allow manufacturers to leverage cloud resources for scalable production, facilitating the transition to smart manufacturing.

IoT and AI convergence in industrial automation drives innovation and efficiency, enabling industries to adapt to modern production demands. Advancements in secure and scalable IIoT networks, coupled with AI-driven optimization strategies, enhance industrial systems' resilience and adaptability, addressing emerging challenges across sectors [84, 46]. This integration improves monitoring and control of processes while addressing security and privacy concerns, ensuring systems leverage real-time data and AI capabilities to optimize performance and maintain operational integrity.

4.5 Environmental and Agricultural Monitoring

IoT integration in environmental and agricultural monitoring enhances data collection and analysis, providing innovative solutions for sustainability and productivity challenges. IoT devices in environmental monitoring enable comprehensive data gathering and support advanced analytical techniques [85]. These technologies facilitate real-time monitoring of environmental parameters, offering critical insights for resource management and conservation efforts.

In agriculture, IoT applications improve productivity and sustainability through precise monitoring of crop conditions, enabling data-driven decisions that optimize resource use and enhance yields [86]. UAV technology integration with IoT systems represents a promising advancement, reducing energy consumption and enhancing monitoring efficiency [87]. UAVs equipped with IoT sensors cover large areas quickly, providing high-resolution data that supports precision agriculture and environmental stewardship.

IoT technologies in environmental and agricultural monitoring revolutionize these sectors by enhancing sustainability and productivity. IoT applications facilitate climate-smart agriculture practices, improve resource management, and enable real-time monitoring of environmental conditions, addressing challenges like climate change and water scarcity. Green IoT initiatives minimize energy consumption and carbon emissions, promoting a sustainable agricultural framework, particularly in regions like Saudi Arabia [69, 85]. By leveraging advanced data collection and analysis, IoT systems enable informed decision-making, fostering adaptive and resilient practices.

4.6 Economic and Societal Impacts

Benchmark	Size	Domain	Task Format	Metric
CVE[88]	5,000	Computer Vision	Image Classification	Consistency Rate, Confidence Level
MEBE[79]	1,000	Edge Computing	Performance Evaluation	CPU Performance, Memory Performance
IoT-Bench[89]	21	Internet OF Things	Platform Evaluation	Stability, Security
DTBM[90]	114,177	Manufacturing	Querying Information And Configuring AI Functions	Response time, Query success rate
AutoDRIVE[91]	1,000,000	Autonomous Driving	Simulation And Real-World Testing	Accuracy, F1-score
CICIoT2023[92]	2,000,000	Cybersecurity	Attack Detection	Accuracy, F1-score
MULTIIOT[93]	1,150,000	Human Activity Recognition	Multimodal Learning	Accuracy, F1-score

Table 3: Table ef presents a comprehensive overview of various benchmarks utilized across different domains such as computer vision, edge computing, and cybersecurity. It details the size, task format, and evaluation metrics associated with each benchmark, providing insights into their application and relevance in AI, IoT, and CPS integration.

The integration of AI, IoT, and CPS has profound economic and societal implications. These technologies drive economic growth by enhancing productivity and efficiency across sectors like manufacturing and healthcare. AI-augmented edge and fog computing optimize resource management, reducing operational costs and fostering innovation [54].

On a societal level, IoT and AI improve quality of life through enhanced services and infrastructure. In smart cities, these technologies enable efficient public services, improving urban living conditions and sustainability. However, ethical challenges require attention to ensure equitable and responsible deployment. Developers' situatedness within socio-technical contexts plays a crucial role in ethical decision-making [94].

IoT and AI's widespread adoption enhances automation and data generation across sectors, raising privacy and data security concerns. Potential data breaches and AI misuse in IoT ecosystems can lead to increased surveillance and diminished trust. Developing robust security protocols and multi-layered approaches is crucial to mitigate risks and protect sensitive information [64, 62]. These issues necessitate frameworks and policies to protect individual rights and ensure technological advancements do not exacerbate social inequalities. The ethical implications underscore the importance of inclusive governance models that consider diverse stakeholder perspectives.

While AI, IoT, and CPS integration presents economic advantages, societal implications require thorough examination. This scrutiny ensures technological advancements are pursued alongside ethical considerations, particularly regarding algorithmic bias and accountability. Balancing these factors fosters responsible innovation and mitigates risks associated with increased autonomy in connected devices [95, 3]. Ongoing research and dialogue are essential to navigate the complex interplay between technology and society, ensuring innovations contribute positively to economic growth and societal well-being. Table 3 illustrates the diverse benchmarks employed in AI, IoT, and CPS research, highlighting their significance in evaluating performance across multiple domains.

5 Challenges and Future Directions

5.1 Challenges and Limitations

The deployment of IoT, AI, and CPS technologies faces significant challenges that impede their full potential. Device heterogeneity in IoT complicates configuration due to diverse communication protocols and data types, requiring robust solutions for sensor discovery and configuration, as current methods are often manual and labor-intensive [9]. Interoperability remains a critical issue due to the lack of standardized APIs for M2M communication and divergent environments [5]. Moreover, the fragmentation of IoT platforms and the need for robust security measures amid evolving threats further complicate deployment [42].

Security and privacy are paramount concerns due to the interconnected nature of IoT devices, amplifying vulnerabilities [42]. Current studies often inadequately address the complexities of managing large-scale IoT networks and the unique security requirements of lightweight devices [25]. The rapid growth of IoT introduces significant security challenges, particularly regarding interoperability and standardized protocols, while implementing blockchain technology in existing infrastructures raises potential operational costs [42]. Additionally, the absence of comprehensive frameworks that integrate all design principles and address the practical challenges of Smart Factories remains a significant barrier [34].

AI and ML applications face challenges from insufficient data quality and integration complexities, underscoring the need for robust security measures to protect sensitive information [93]. The deployment of edge devices in IoT systems faces scalability challenges, requiring robust infrastructure to support widespread implementation [9]. High latency in cloud communications and dependence on continuous connectivity also pose primary challenges in fog computing architectures [5].

AGI is hindered by the inability to address all potential pathways to dangerous AI, leaving some scenarios unmanageable [17]. Simplifying human preferences into a one-dimensional normal distribution may fail to capture the complexity of actual user preferences, posing limitations in human-AI interaction models [16].

The Internet of People (IoP) introduces complexities in integrating human behavioral models into network design, complicating protocol implementation and the integration of human-centric approaches into digital networks [8]. The virtualization of robots for search and rescue operations presents challenges in maintaining consistent node-level virtualization across diverse IoT resources [43].

In cloud services, the lack of standardized definitions for optimization indicators and the complexity of selecting suitable services considering various performance factors pose significant challenges [37]. The reliance on semantic metadata for service composition can also limit effectiveness, as such metadata may not always be available [96].

Addressing these challenges requires developing comprehensive frameworks and solutions to enhance interoperability, security, and data management while meeting the unique demands of emerging technologies like IoT and 5G. This involves creating robust regulatory policies to facilitate investment and innovation, integrating advanced networking and virtualization techniques for secure applications, particularly in healthcare. Leveraging tools such as Blockchain and M2M messaging can improve data management and mitigate risks associated with technological advancements [75, 21]. Future research must focus on leveraging social relationships for improved service discovery and ensuring reliable real-time monitoring across diverse contexts.

5.2 Security and Privacy Considerations

The integration of IoT, AI, and CPS into various domains presents a complex landscape of security and privacy challenges that necessitate comprehensive strategies for safe deployment. The emergence of new hacking methods and malware-as-a-service highlights the evolving nature of cybersecurity risks in IoT environments [97], necessitating robust cybersecurity measures against these advanced threats.

Governance of advanced AI systems is crucial for managing security and privacy considerations, emphasizing proactive governance and technical research and development (RD) to mitigate risks [38]. The deployment of smart grid technologies underscores the need for stringent cybersecurity and privacy measures to protect sensitive data and ensure system integrity [6].

Integrating various IoT devices into cohesive systems, such as those used in advertising strategies, introduces privacy concerns related to user data collection [73]. The incorporation of IoT capabilities into Cyber-Physical Social Machines (CPSMs) enhances automation and user engagement but also raises new security and privacy concerns that must be addressed [18].

Generative AI in IoT poses significant security challenges, necessitating proactive security strategies to safeguard these technologies [42]. Additionally, training AI systems on diverse datasets is essential to avoid bias and ensure that these systems do not inadvertently compromise user privacy or security [11].

The security and privacy considerations in these interconnected technologies demand a multi-faceted approach incorporating technical safeguards, ethical guidelines, and regulatory innovations. Such an approach is crucial for safeguarding user data against potential breaches, fostering trust in the rapidly evolving landscape of IoT and AI applications, and facilitating the secure and ethical implementation of these transformative technologies. Developing robust security protocols and adopting multi-layered strategies will address the unique challenges posed by the convergence of generative AI and IoT, ensuring that these innovations enhance rather than compromise privacy and safety in AI-driven environments [52, 64, 42, 3].

5.3 Ethical and Societal Implications

The integration of advanced technologies such as AI, IoT, and generative AI models into various sectors presents profound ethical and societal challenges. The ethical landscape of these technologies is characterized by issues related to transparency, privacy, and the socio-economic impacts of automation [98]. The context of IoT applications is critical for determining ethical behavior, highlighting the need for context-aware ethical frameworks [99].

A significant ethical concern is the potential for digital surveillance, where the pervasive monitoring capabilities of IoT devices can infringe on individual privacy and autonomy. This necessitates transparency in algorithmic decision-making to ensure users are aware of how their data is used, fostering trust in these systems [98]. The IoP framework emphasizes addressing privacy and trust issues in data management, highlighting the need for robust privacy-preserving mechanisms [31].

The socio-economic impacts of automation driven by AI and IoT present another layer of ethical complexity, as automation can lead to significant labor market shifts, necessitating careful examination of the socio-economic implications to ensure equitable distribution of benefits [98]. While AI has the potential to enhance creativity and social interactions, current methods may not fully account for the psycho-social dynamics influencing these outcomes [19].

Developing ethical guidelines and frameworks is crucial to mitigate risks associated with the rapid advancement of AI technologies. These frameworks must prioritize ethical considerations in AI deployment, ensuring alignment with societal values and contributing positively to social welfare [98]. Addressing these ethical and societal challenges requires a multifaceted approach that incorporates ethical guidelines, transparent governance, and active community involvement, fostering a technology landscape that aligns with collective human values and goals.

5.4 Future Directions and Research Opportunities

The rapidly evolving technological landscape, characterized by the convergence of IoT, AI, and CPS, presents numerous avenues for future research aimed at addressing current challenges and maximizing the potential of these transformative technologies. A critical area for exploration is enhancing interoperability and security within IoT environments. Future research should focus on developing scalable and adaptive security solutions while exploring emerging trends in IoT interoperability and management [25]. Standardizing protocols and APIs for M2M communication is essential for ensuring seamless integration across diverse systems, while leveraging emerging trends in machine learning and control engineering can bolster security measures [42].

In IoT security, expanding datasets to include a broader range of attack types and refining methodologies for analyzing security vulnerabilities are crucial research directions. The exploration of adaptive security measures capable of dynamically responding to evolving threats will enhance the resilience of IoT systems. Moreover, enhancing the interoperability of Green IoT technologies, exploring new

energy sources, and developing innovative solutions for reducing CO2 emissions are vital areas for future research [26].

Integrating IoT into Human Resource Development (HRD) presents opportunities for developing robust frameworks that leverage emerging technologies to enhance workforce development. Future research should explore the implications of these technologies for HRD, particularly regarding skill development and workforce adaptability. Additionally, developing standardized datasets, enhancing theoretical analyses, and applying reinforcement learning in complex manufacturing environments are promising research directions [37].

Future research should also investigate optimizing peer recommendations and the long-term impacts of AI-driven systems on creativity [19]. In IoFT environments, robust algorithms capable of handling heterogeneous data distributions and improving communication efficiency are essential [39]. Additionally, refining algorithms for each step of the IoT Process Awareness Framework and exploring its applicability in domains such as healthcare can provide valuable insights for future applications [14].

The Industrial Metaverse presents significant research opportunities, particularly in developing standardized protocols for interoperability and enhancing security mechanisms. Innovative training solutions and inclusive hiring practices are essential for bridging the skills gap in the context of the 4th Industrial Revolution, focusing on traditionally underrepresented populations. Future research directions could explore contract designs accommodating bounded rationality in user behavior and developing online learning approaches for dynamic contract adjustments [28].

Furthermore, future research should expand benchmarks to include additional metrics and dimensions reflecting the evolving nature of AI in business applications [24]. Proposing future research directions focusing on developing efficient AI algorithms and enhancing data collection methods for real-time applications in 5G networks can significantly contribute to advancing these technologies [23].

These research directions underscore the importance of continued innovation and interdisciplinary collaboration to address existing challenges and harness the opportunities presented by these interconnected technologies. By implementing advanced technologies such as AI, edge computing, and 5G networks, we can create a future that is not only more intelligent and secure but also seamlessly interconnected, enabling real-time applications across various sectors, including healthcare, education, and disaster recovery, while fostering innovation and investment in essential infrastructure [51, 100, 3, 21].

6 Conclusion

The integration of technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), Cyber-Physical Systems (CPS), and smart environments has been shown to significantly enhance human-computer interactions and automate complex processes across various domains, fostering adaptive environments that contribute to economic growth and societal well-being. This convergence highlights the critical need for interdisciplinary collaboration to develop robust security specifications and protocols tailored to the unique challenges presented by IoT. The evolution of the Internet of People (IoP) paradigm is pivotal in addressing challenges posed by Cyber-Physical Convergence and provides a framework for future research and development in networking.

The survey underscores the importance of adaptive resilience mechanisms to address the evolving nature of IoT systems, integrating security measures to ensure long-term dependability. A comprehensive approach involving policymakers, industry standards, and international cooperation is essential for enhancing IIoT security. Integrating semantic communication with edge intelligence offers significant improvements in communication efficiency, providing a foundation for future research directions. Additionally, the exploration of Reconfigurable Intelligent Surfaces (RIS) presents a promising avenue for enhancing connectivity and signal quality across challenging environments.

Despite significant advancements, substantial challenges remain, necessitating ongoing research and development. The survey highlights the need to address statistical heterogeneity and the benefits of decentralized learning, particularly within the Internet of Federated Things (IoFT), which can revolutionize industries through collaborative model training without compromising privacy. While generative AI offers productivity enhancements, it also poses risks of homogenization and bias, necessitating careful consideration of its societal implications.

Continued research and development are imperative to address these challenges and harness the opportunities presented by interconnected technologies. By fostering interdisciplinary collaboration and adopting responsible practices, these innovations can contribute positively to societal advancement and economic prosperity. Future research should focus on structured approaches to evaluate the impacts of interface designs on user interactions with AI systems, ensuring alignment with human values and enhancing user experiences. The value entropy model provides valuable insights for intervention strategies and decision-making in service ecosystem management, emphasizing the importance of strategic planning in deploying these technologies.

References

[1] Stefanie Krause, Bhumi Hitesh Panchal, and Nikhil Ubhe. The evolution of learning: Assessing the transformative impact of generative ai on higher education, 2024.

[2] Kai Li, Yingping Cui, Weicai Li, Tiejun Lv, Xin Yuan, Shenghong Li, Wei Ni, Meryem Simsek, and Falko Dressler. When internet of things meets metaverse: Convergence of physical and cyber worlds, 2022.

[3] Mehrdad Maghsoudi, Reza Nourbakhsh, Mehrdad Agha Mohammadali Kermani, and Rahim Khanizad. The power of patents: Leveraging text mining and social network analysis to forecast iot trends, 2023.

[4] Jim Hahn. The bibliotelemetry of information and environment: an evaluation of iot-powered recommender systems, 2018.

[5] Badraddin Alturki, Stephan Reiff-Marganiec, Charith Perera, and Suparna De. Exploring the effectiveness of service decomposition in fog computing architecture for the internet of things, 2019.

[6] Yuanjie Liu, Xiongping Yang, Wenkun Wen, and Minghua Xia. Smarter grid in the 5g era: A framework integrating power internet of things with a cyber physical system. *Frontiers in Communications and Networks*, 2:689590, 2021.

[7] Jan Seeger, Rohit A. Deshmukh, Vasil Sarafov, and Arne Bröring. Dynamic iot choreographies, 2019.

[8] Eric Monteiro and Elena Parmiggiani. Synthetic knowing: The politics of the internet of things, 2019.

[9] Muhammad Junaid Farooq and Quanyan Zhu. Phd forum: Enabling autonomic iot for smart urban services, 2019.

[10] Katelyn Morrison, Shamsi Iqbal, and Eric Horvitz. Ai-powered reminders for collaborative tasks: Experiences and futures, 2024.

[11] Francisco Castro, Jian Gao, and Sébastien Martin. Human-ai interactions and societal pitfalls, 2023.

[12] Mary Ann Weitnauer, Jennifer Rexford, Nicholas Laneman, Matthieu Bloch, Santiago Griljava, Catherine Ross, and Gee-Kung Chang. Smart wireless communication is the cornerstone of smart infrastructures, 2017.

[13] Charith Perera, Prem Jayaraman, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. Context-aware dynamic discovery and configuration of 'things' in smart environments, 2013.

[14] Juergen Mangler, Ronny Seiger, Janik-Vasily Benzin, Joscha Grüger, Yusuf Kirikkayis, Florian Gallik, Lukas Malburg, Matthias Ehrendorfer, Yannis Bertrand, Marco Franceschetti, Barbara Weber, Stefanie Rinderle-Ma, Ralph Bergmann, Estefanía Serral Asensio, and Manfred Reichert. From internet of things data to business processes: Challenges and a framework, 2024.

[15] Mir Sajjad Hussain Talpur. The appliance pervasive of internet of things in healthcare systems, 2013.

[16] Oded Nov, Yindalon Aphinyanaphongs, Yvonne W. Lui, Devin Mann, Maurizio Porfiri, Mark Riedl, John-Ross Rizzo, and Batia Wiesenfeld. The transformation of patient-clinician relationships with ai-based medical advice: A "bring your own algorithm" era in healthcare, 2020.

[17] Feng Liu, Yong Shi, and Ying Liu. Intelligence quotient and intelligence grade of artificial intelligence, 2017.

[18] Aastha Madaan, Jason R. C. Nurse, David De Roure, Kieron O'Hara, Wendy Hall, and Sadie Creese. A storm in an iot cup: The emergence of cyber-physical social machines, 2018.

[19] Raiyan Abdul Baten, Ali Sarosh Bangash, Krish Veera, Gourab Ghoshal, and Ehsan Hoque. Ai can enhance creativity in social networks, 2024.

[20] Zhenchang Xing, Qing Huang, Yu Cheng, Liming Zhu, Qinghua Lu, and Xiwei Xu. Prompt sapper: Llm-empowered software engineering infrastructure for ai-native services, 2023.

[21] Olena Cherniaieva, Olena Orlenko, and Oleksandra Ashcheulova. The infrastructure of the internet services market of the future: analysis of formation problems. *Futurity Economics&Law*, 3(1):4–27, 2023.

[22] Savannah Thais. Misrepresented technological solutions in imagined futures: The origins and dangers of ai hype in the research community, 2024.

[23] Youness Arjoune and Saleh Faruque. Artificial intelligence for 5g wireless systems: Opportunities, challenges, and future research directions, 2020.

[24] Moshe BenBassat. Aiq: Measuring intelligence of business ai software, 2018.

[25] Mahmoud Elkhodr, Seyed Shahrestani, and Hon Cheung. The internet of things: New interoperability, management and security challenges, 2016.

[26] Jose Macias, Harold Pinilla, Wilder Castellanos, Jose Alvarado, and Andres Sánchez. Design and implementation of a multiprotocol iot gateway, 2020.

[27] Huansheng Ning, Zhong Zhen, Feifei Shi, and Mahmoud Daneshmand. A survey of identity modeling and identity addressing in internet of things. *IEEE Internet of Things Journal*, 7(6):4697–4710, 2020.

[28] Juntao Chen, Junaid Farooq, and Quanyan Zhu. Qos based contract design for profit maximization in iot-enabled data markets, 2023.

[29] Xiao Xue, Zhaojie Chen, Shufang Wang, Zhiyong Feng, Yucong Duan, and Zhangbing Zhou. Value entropy model: Metric method of service ecosystem evolution, 2020.

[30] Miroslav Bures, Pavel Blazek, Jiri Nema, and Hynek Schvach. Factors impacting resilience of internet of things systems in critical infrastructure, 2022.

[31] Marco Conti and Andrea Passarella. The internet of people: A human and data-centric paradigm for the next generation internet, 2022.

[32] Feifei Shi, Wenxi Wang, Hang Wang, and Huansheng Ning. The internet of people: A survey and tutorial, 2021.

[33] Matteo Mordacchini, Marco Conti, Andrea Passarella, and Raffaele Bruno. Human-centric data dissemination in the iop: Large-scale modeling and evaluation, 2021.

[34] Alfonso Di Pace, Giuseppe Fenza, Mariacristina Gallo, Vincenzo Loia, Aldo Meglio, and Francesco Orciuoli. Implementing the cognition level for industry 4.0 by integrating augmented reality and manufacturing execution systems, 2020.

[35] Iván Alfonso, Kelly Garcés, Harold Castro, and Jordi Cabot. Self-adaptive architectures in iot systems: A systematic literature review, 2021.

[36] Erkan Karabulut, Salvatore F. Pileggi, Paul Groth, and Victoria Degeler. Ontologies in digital twins: A systematic literature review, 2023.

[37] Cuixia Li, Liqiang Liu, and Li Shi. Review of cloud service composition for intelligent manufacturing, 2024.

[38] Yoshua Bengio, Geoffrey Hinton, Andrew Yao, Dawn Song, Pieter Abbeel, Trevor Darrell, Yuval Noah Harari, Ya-Qin Zhang, Lan Xue, Shai Shalev-Shwartz, Gillian Hadfield, Jeff Clune, Tegan Maharaj, Frank Hutter, Atılım Güneş Baydin, Sheila McIlraith, Qiqi Gao, Ashwin Acharya, David Krueger, Anca Dragan, Philip Torr, Stuart Russell, Daniel Kahneman, Jan Brauner, and Sören Mindermann. Managing extreme ai risks amid rapid progress, 2024.

[39] Raed Kontar, Naichen Shi, Xubo Yue, Seokhyun Chung, Eunshin Byon, Mosharaf Chowdhury, Judy Jin, Wissam Kontar, Neda Masoud, Maher Noueihed, Chinedum E. Okwudire, Garvesh Raskutti, Romesh Saigal, Karandeep Singh, and Zhisheng Ye. The internet of federated things (ioft): A vision for the future and in-depth survey of data-driven approaches for federated learning, 2021.

[40] A Akanbi. Towards a microservice-based middleware for a multi-hazard early warning system, 2023.

[41] Panagiotis Fountas, Kostas Kolomvatsos, and Christos Anagnostopoulos. Data synopses management based on a deep learning model, 2020.

[42] Honghui Xu, Yingshu Li, Olusesi Balogun, Shaoen Wu, Yue Wang, and Zhipeng Cai. Security risks concerns of generative ai in the iot, 2024.

[43] Junjie Li, Kang Li, Dewei Han, Jian Xu, and Zhaoyuan Ma. Amplifying robotics capacities with a human touch: An immersive low-latency panoramic remote system, 2024.

[44] Hawzhin Mohammed, Tolulope A. Odetola, Nan Guo, and Syed Rafay Hasan. Dynamic distribution of edge intelligence at the node level for internet of things, 2021.

[45] Usman Tariq, Irfan Ahmed, Ali Kashif Bashir, and Kamran Shaukat. A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review. *Sensors*, 23(8):4117, 2023.

[46] Hussain Al-Aqrabi and Richard Hill. A secure connectivity model for internet of things analytics service delivery, 2019.

[47] Elias G Carayannis, Klitos Christodoulou, Panayiotis Christodoulou, Savvas A Chatzichristofis, and Zinon Zinonos. Known unknowns in an era of technological and viral disruptions—implications for theory, policy, and practice. *Journal of the knowledge economy*, pages 1–24, 2021.

[48] Mohab Aly, Foutse Khomh, Yann-Gaël Guéhéneuc, Hironori Washizaki, and Soumaya Yacout. Is fragmentation a threat to the success of the internet of things?, 2018.

[49] Lin Zhang, Ying-Chang Liang, and Dusit Niyato. 6g visions: Mobile ultra-broadband, super internet-of-things, and artificial intelligence. *China Communications*, 16(8):1–14, 2019.

[50] Kim J. L. Nevelsteen, Theo Kanter, and Rahim Rahmani. Comparing properties of massively multiplayer online worlds and the internet of things, 2016.

[51] Elisa Bertino and Sujata Banerjee. Artificial intelligence at the edge, 2020.

[52] Emna Baccour, Naram Mhaisen, Alaa Awad Abdellatif, Aiman Erbad, Amr Mohamed, Mounir Hamdi, and Mohsen Guizani. Pervasive ai for iot applications: A survey on resource-efficient distributed artificial intelligence, 2022.

[53] Khaled Alanezi and Shivakant Mishra. An edge-based architecture to support the execution of ambience intelligence tasks using the iop paradigm, 2020.

[54] Shreshth Tuli, Fatemeh Mirhakimi, Samodha Pallewatta, Syed Zawad, Giuliano Casale, Bahman Javadi, Feng Yan, Rajkumar Buyya, and Nicholas R. Jennings. Ai augmented edge and fog computing: Trends and challenges, 2023.

[55] Stefanos Laskaridis, Stylianos I. Venieris, Alexandros Kouris, Rui Li, and Nicholas D. Lane. The future of consumer edge-ai computing, 2024.

[56] Georg Rehm, Dimitrios Galanis, Penny Labropoulou, Stelios Piperidis, Martin Welß, Ricardo Usbeck, Joachim Köhler, Miltos Deligiannis, Katerina Gkirtzou, Johannes Fischer, Christian Chiarcos, Nils Feldhus, Julián Moreno-Schneider, Florian Kintzel, Elena Montiel, Víctor Rodríguez Doncel, John P. McCrae, David Laqua, Irina Patricia Theile, Christian Dittmar, Kalina Bontcheva, Ian Roberts, Andrejs Vasiljevs, and Andis Lagzdiņš. Towards an interoperable ecosystem of ai and lt platforms: A roadmap for the implementation of different levels of interoperability, 2020.

[57] Ketai Qiu, Niccolò Puccinelli, Matteo Ciniselli, and Luca Di Grazia. From today's code to tomorrow's symphony: The ai transformation of developer's routine by 2030, 2024.

[58] Prasant Misra, Yogesh Simmhan, and Jay Warrior. Towards a practical architecture for the next generation internet of things, 2016.

[59] Dominik Martin, Niklas Kühl, and Marcel Schwenk. Towards a reference architecture for future industrial internet of things networks, 2021.

[60] Yongrui Qin, Quan Z. Sheng, Nickolas J. G. Falkner, Schahram Dustdar, Hua Wang, and Athanasios V. Vasilakos. When things matter: A data-centric view of the internet of things, 2014.

[61] Rakhi Misuriya Gupta. Intelligent data in the context of the internet-of-things, 2015.

[62] Ons Aouedi, Thai-Hoc Vu, Alessio Sacco, Dinh C. Nguyen, Kandaraj Piamrat, Guido Marchetto, and Quoc-Viet Pham. A survey on intelligent internet of things: Applications, security, privacy, and future directions, 2024.

[63] Parushi Malhotra, Yashwant Singh, Pooja Anand, Deep Kumar Bangotra, Pradeep Kumar Singh, and Wei-Chiang Hong. Internet of things: Evolution, concerns and security challenges. *Sensors*, 21(5):1809, 2021.

[64] Earlence Fernandes, Amir Rahmati, Kevin Eykholt, and Atul Prakash. Internet of things security research: A rehash of old ideas or new intellectual challenges?, 2017.

[65] Aya Sayed, Yassine Himeur, Abdullah Alsalemi, Faycal Bensaali, and Abbes Amira. Intelligent edge-based recommender system for internet of energy applications, 2021.

[66] Li Yang and Abdallah Shami. Iot data analytics in dynamic environments: From an automated machine learning perspective, 2022.

[67] Charith Perera, Prem Jayaraman, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. Dynamic configuration of sensors using mobile sensor hub in internet of things paradigm, 2013.

[68] Haya Elayan, Moayad Aloqaily, Fakhri Karray, and Mohsen Guizani. Internet of behavior (iob) and explainable ai systems for influencing iot behavior, 2022.

[69] Muhammad Shoaib Farooq, Shamyla Riaz, and Atif Alvi. Web of things and trends in agriculture: A systematic literature review, 2023.

[70] Yasar Majib and Charith Perera. Context aware family dynamics based internet of things access control towards better child safety, 2019.

[71] Charith Perera, Prem Prakash Jayaraman, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. Sensor discovery and configuration framework for the internet of things paradigm, 2013.

[72] Mustafa Emara, Hesham ElSawy, and Gerhard Bauch. A spatiotemporal framework for information freshness in iot uplink networks, 2020.

[73] Hidayet Aksu, Leonardo Babun, Mauro Conti, Gabriele Tolomei, and A. Selcuk Uluagac. Advertising in the iot era: Vision and challenges, 2018.

[74] Seung Yeob Shin, Shiva Nejati, Mehrdad Sabetzadeh, Lionel C. Briand, Chetan Arora, and Frank Zimmer. Dynamic adaptation of software-defined networks for iot systems: A search-based approach, 2020.

[75] Mohammad A. Salahuddin, Ala Al-Fuqaha, Mohsen Guizani, Khaled Shuaib, and Farag Sallabi. Softwarization of internet of things infrastructure for secure and smart healthcare, 2018.

[76] Mirza Akhi Khatun, Sanober Farheen Memon, Ciarán Eising, and Lubna Luxmi Dhirani. Machine learning for healthcare-iot security: A review and risk mitigation, 2024.

[77] Jiayuan Chen, You Shi, Changyan Yi, Hongyang Du, Jiawen Kang, and Dusit Niyato. Generative ai-driven human digital twin in iot-healthcare: A comprehensive survey, 2024.

[78] Giuliano Cornacchia, Mirco Nanni, Dino Pedreschi, and Luca Pappalardo. Navigation services amplify concentration of traffic and emissions in our cities, 2024.

[79] Qian Qu, Ronghua Xu, Seyed Yahya Nikouei, and Yu Chen. An experimental study on microservices based edge computing platforms, 2020.

[80] Ana L. C. Bazzan, Anderson R. Tavares, André G. Pereira, Cláudio R. Jung, Jacob Scharcanski, Joel Luis Carbonera, Luís C. Lamb, Mariana Recamonde-Mendoza, Thiago L. T. da Silveira, and Viviane Moreira. "a nova eletricidade: Aplicações, riscos e tendências da ia moderna – "the new electricity": Applications, risks, and trends in current ai, 2023.

[81] Huimei Han, Wenchao Zhai, and Jun Zhao. Smart city enabled by 5g/6g networks: An intelligent hybrid random access scheme, 2022.

[82] Dmitry Namiot and Manfred Schneps-Schneppe. Smart cities software from the developer's point of view, 2013.

[83] Misty Blowers, Jose Iribarne, Edward Colbert, and Alexander Kott. The future internet of things and security of its control systems, 2016.

[84] Bassam Zahran, Adamu Hussaini, and Aisha Ali-Gombe. Security of it/ot convergence: Design and implementation challenges, 2023.

[85] Andreas Kamilaris and Frank Ostermann. Geospatial analysis and internet of things in environmental informatics, 2018.

[86] Manal Alshehri and Ohoud Alharbi. Understanding the landscape of leveraging iot for sustainable growth in saudi arabia, 2024.

[87] S. H. Alsamhi, Ou Ma, M. Samar Ansari, and Qingliang Meng. Greening internet of things for smart everythings with a green-environment life: A survey and future prospects, 2018.

[88] Alex Cummaudo, Rajesh Vasa, John Grundy, Mohamed Abdelrazek, and Andrew Cain. Losing confidence in quality: Unspoken evolution of computer vision services, 2019.

[89] Mehar Ullah, Pedro H. J. Nardelli, Annika Wolff, and Kari Smolander. Twenty-one key factors to choose an iot platform: Theoretical framework and its applications, 2020.

[90] Joern Ploennigs, Konstantinos Semertzidis, Fabio Lorenzi, and Nandana Mihindukulasooriya. Scaling knowledge graphs for automating ai of digital twins, 2022.

[91] Tanmay Vilas Samak, Chinmay Vilas Samak, Sivanathan Kandhasamy, Venkat Krovi, and Ming Xie. Autodrive: A comprehensive, flexible and integrated digital twin ecosystem for enhancing autonomous driving research and education, 2023.

[92] Neelam Patidar, Sally Zreiqat, Sirisha Mahesh, and Jongwook Woo. Cyberattack data analysis in iot environments using big data, 2024.

[93] Shentong Mo, Louis-Philippe Morency, Russ Salakhutdinov, and Paul Pu Liang. Multiiot: Benchmarking machine learning for the internet of things, 2024.

[94] Funda Ustek-Spilda, Alison Powell, Irina Shklovski, and Sebastian Lehuede. Peril v. promise: Iot and the ethical imaginaries, 2019.

[95] Michael Chui, Mark Collins, and Mark Patel. The internet of things: Catching up to an accelerating opportunity. 2021.

[96] Darko Andročec. Using json-ld to compose different iot and cloud services, 2018.

[97] Tyson Brooks. The professionalization of the hacker industry, 2022.

[98] Ovidiu Vermesan and Joël Bacquet. *Cognitive Hyperconnected Digital Transformation: Internet of Things Intelligence Evolution*. CRC Press, 2022.

[99] Seng W. Loke. Achieving ethical algorithmic behaviour in the internet-of-things: a review, 2019.

[100] Shoumen Palit Austin Datta. Intelligence in artificial intelligence, 2016.

Disclaimer:

SurveyX is an AI-powered system designed to automate the generation of surveys. While it aims to produce high-quality, coherent, and comprehensive surveys with accurate citations, the final output is derived from the AI's synthesis of pre-processed materials, which may contain limitations or inaccuracies. As such, the generated content should not be used for academic publication or formal submissions and must be independently reviewed and verified. The developers of SurveyX do not assume responsibility for any errors or consequences arising from the use of the generated surveys.