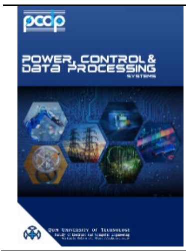
DOI: 10.30511/pcdp.2026.2086308.1066 - ISSN: 3060-8376 - Vol 3(2), 2026



POWER, CONTROL AND DATA PROCESSING SYSTEMS

Available Online at: https://pcdp.qut.ac.ir/

Strategic Convergence of Artificial Intelligence, Blockchain, and Internet of Things in Shaping Industry 5.0 and Next-Generation Smart Cities: An Advanced Systematic Review

ARTICLE INFO

Article Type
Original Research

Authors
Alireza joshan[1,*]

[1] Master of Science in Electrical Power Engineering, Faculty of Electrical Engineering, University of Guilan, Guilan, Iran, Alireza.joshan.guilan@gmail.com

**** Correspondence***
Address: Department of electrical engineering, University of Guilan, guilan, Iran.
Phone: -
Fax: -
Alireza.joshan.guilan@gmail.com

Article History
Received: February 02, 2026
Accepted: May 08, 2026
ePublished: June 01, 2026

ABSTRACT

The convergence of Artificial Intelligence (AI), Blockchain, and the Internet of Things (IoT) has emerged as a pivotal enabler for Industry 5.0 and next-generation smart city infrastructures. This study presents a PRISMA-guided systematic review of 82 peer-reviewed articles published between 2015 and 2025, retrieved from Scopus, Web of Science, IEEE Xplore, ScienceDirect, and SpringerLink. The analysis highlights a dominant layered architecture in which IoT facilitates real-time data acquisition, Blockchain ensures decentralized security, transparency, and trust, and AI supports intelligent analytics and autonomous decision-making. Beyond synthesizing existing research, this study proposes a unified taxonomy of AI–Blockchain–IoT integration models, identifies critical research gaps, and outlines a conceptual roadmap for scalable, human-centric implementations in industrial and urban environments. Despite rapid advancements, challenges such as interoperability, energy efficiency, latency, scalability, and the lack of unified standards remain significant barriers to large-scale deployment. The findings provide actionable insights and strategic guidance for developing secure, efficient, and deployable integrated frameworks for real-world applications.

Keywords: Artificial Intelligence, Blockchain, Internet of Things, Industry 5.0, Smart Cities

1 Introduction

With the rapid advancement of emerging technologies, the concepts of Industry 5.0 and smart cities have become central to digital transformation in both industrial and urban domains [1,2]. Industry 5.0 goes beyond mere automation and smart manufacturing, emphasizing human-machine collaboration, intelligent automation, and system sustainability, requiring infrastructures that integrate advanced technologies such as Artificial Intelligence (AI), Blockchain, and the Internet of Things (IoT) [3,4]. The convergence of these three technologies enables the creation of autonomous, secure, scalable, and flexible systems in industrial and urban environments; however, technical, operational, and standardization challenges continue to hinder full implementation [5,6].

The chronology and key components of industrial advancements are displayed in Fig. 1. where the latest and cutting-edge phase in the evolution of industry and production technology is Industry 5.0 referred to as The Fifth Industrial Revolution. Industry 5.0 builds upon the foundations of its predecessors while introducing groundbreaking advancements that emphasize the harmonious interaction between humans and machines. The core of Industry 5.0 is the concept of "human-machine collaboration [1,92].

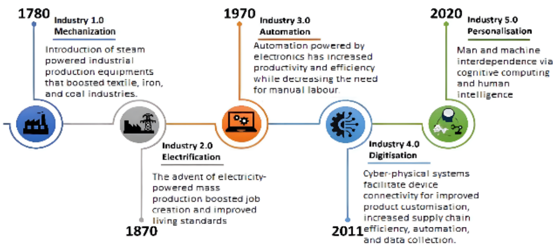


Fig1.Timeline and essentials of industrial revolutions

Previous studies have mostly addressed each technology separately. Some have focused on AI applications in industrial and urban data analytics [7], others on security and trust in blockchain networks [8], and some on optimizing real-time data collection and processing in IoT [9]. This fragmentation has resulted in the absence of a comprehensive and practical framework for the integrated convergence of these technologies. In other words, the primary research gap lies in the practical integration of AI, Blockchain, and IoT within Industry 5.0 and smart city infrastructures, which current studies have not systematically and operationally addressed [10].

In response to this gap, the novelty of the present study lies in providing a systematic and practical review that analyzes and categorizes frameworks, models, and operational approaches for AI–Blockchain–IoT convergence in the development of Industry 5.0 and smart city infrastructures. This review enables the identification of implementation challenges, optimization strategies, future research directions, and practical criteria for designing deployable frameworks [11,12].

The central research question driving this study is: How can technical and practical frameworks for the convergence of Artificial Intelligence (AI), Blockchain, and the Internet of Things (IoT) be systematically designed and rigorously evaluated to facilitate the advancement of Industry 5.0 and smart city infrastructures?

To address this complex inquiry, this article undertakes a comprehensive systematic review of existing literature and frameworks. It critically identifies prevailing gaps, technical limitations, and integration challenges, subsequently proposing innovative and actionable pathways for the development of next-generation intelligent infrastructures. The paper is structured to guide the reader through a logical progression from methodological foundations to strategic recommendations, as detailed below:

Section II delineates the research methodology employed in this study. It provides a transparent account of the systematic review protocol, including the search strategies, database selection, and strict inclusion and exclusion criteria used to curate the relevant body of knowledge. This section ensures the reproducibility and academic rigor of the review process.

Section III offers an in-depth overview of the three pivotal enabling technologies: Artificial Intelligence, Blockchain, and the Internet of Things. It elucidates their foundational concepts, operational mechanisms, and distinct yet complementary roles within the evolving ecosystems of Industry 5.0 and smart cities. This section establishes the theoretical groundwork for understanding how these technologies interact to create synergistic value.

Section IV presents a critical review and categorization of existing frameworks dedicated to the convergence of AI, Blockchain, and IoT. It highlights various architectural models and integration strategies, analyzing their structural components and functional capabilities. This analysis serves to map the current landscape of converged technological solutions. Section V delivers a comprehensive analysis and comparative discussion of the findings derived from the systematic review. It systematically identifies the strengths of current approaches, acknowledges their inherent limitations, and pinpoints specific research gaps that remain unaddressed in the existing literature. This critical evaluation forms the basis for the study's contributions.

Section VI proposes a strategic roadmap for future research and practical implementation. It outlines key technical priorities, scalability considerations, and policy implications necessary to bridge the gap between theoretical frameworks and real-world deployment. This section aims to provide stakeholders with a clear direction for advancing the field.

Finally, Section VII concludes the paper by summarizing the main contributions of the study, reflecting on the implications of the findings, and presenting directions for future research. It reinforces the significance of the proposed frameworks in shaping the future of intelligent, sustainable, and human-centric industrial and urban environments.

2 Methodology

This section describes the research approach, literature search strategy, inclusion and exclusion criteria, data extraction, and framework analysis used for conducting a systematic review of frameworks for the convergence of Artificial Intelligence (AI), Blockchain, and the Internet of Things (IoT) in the development of Industry 5.0 and smart city infrastructures**.** The main objective is to provide a transparent, replicable, and practical structure for collecting and analyzing scientific evidence.

2.1 Systematic Review Protocol

This systematic review was conducted in strict accordance with the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines to ensure transparency, methodological rigor, and reproducibility. The research protocol encompasses a comprehensive process beginning with the definition of the research question and study objectives, followed by the identification of relevant keywords and the selection of reputable databases. Subsequently, articles were screened and selected based on predefined inclusion and exclusion criteria. Key data were then extracted and analyzed to evaluate existing frameworks. Finally, the findings were synthesized, research gaps were identified, and practical pathways for future development were proposed.

Main Research Question:

How can technical and practical frameworks for the convergence of Artificial Intelligence, Blockchain, and the Internet of Things be systematically designed and evaluated to facilitate the development of Industry 5.0 and smart city infrastructures?

2.2 Literature Search Strategy

To ensure a comprehensive and robust literature review, the search strategy was meticulously designed by integrating subject-specific keywords with advanced Boolean operators. This approach was applied across four leading international academic databases: IEEE Xplore, ScienceDirect, SpringerLink, and Scopus, thereby maximizing the coverage of relevant scholarly works. The core search terms focused on the key technological pillars and application domains, specifically "Artificial Intelligence," "Blockchain," "Internet of Things," "Industry 5.0," and "Smart City." Furthermore, the temporal scope of the search was limited to publications from 2015 to 2025. This specific timeframe was chosen to capture the most recent technological advancements and to ensure that the identified frameworks remain operationally relevant and reflective of the current state of the art in these rapidly evolving fields.

2.3 Inclusion and Exclusion Criteria

Inclusion Criteria:

The selection of literature was strictly guided by a set of predefined inclusion criteria to ensure the relevance and quality of the analyzed studies. First, the articles had to explicitly address the convergence of Artificial Intelligence, Blockchain, and the Internet of Things within the context of industrial and urban infrastructures. Second, only works published in reputable peer-reviewed journals and recognized academic conferences were considered, thereby guaranteeing the scientific rigor of the sources. Finally, the selected studies were required to provide tangible contributions in the form of operational frameworks, theoretical models, or practical implementations, ensuring that the review focuses on actionable insights rather than purely theoretical discussions.

Exclusion Criteria:

To maintain the focus on practical and current advancements, specific exclusion criteria were applied to filter out less relevant or outdated materials. Studies that were purely theoretical or educational in nature, lacking any practical frameworks or operational models, were excluded to ensure the review remained grounded in actionable insights. Additionally, articles published prior to 2015 were omitted, as they would not reflect the rapid technological evolution and recent developments in the convergence of AI, Blockchain, and IoT. Finally, duplicate studies and those lacking sufficient operational analysis were removed to avoid redundancy and to ensure that each included paper contributed unique and substantive value to the synthesis of findings.

2.4 Article Selection Process and Data Extraction

The article selection process was rigorously conducted following the standard PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines, ensuring a transparent and reproducible methodology through several distinct stages. Initially, in the identification phase, a comprehensive search across major databases including IEEE Xplore, ScienceDirect, SpringerLink, and Scopus yielded a total of 350 relevant articles. To ensure the uniqueness of the dataset, 120 duplicate or highly similar articles were identified and excluded, leaving 230 distinct studies for further evaluation.

Subsequently, a rigorous screening of titles and abstracts was performed to assess relevance and operational focus. During this step, 148 articles were deemed insufficiently aligned with the study's objectives and were removed, resulting in a refined pool of 82 articles selected for full-text assessment. In the next stage, all 82 remaining articles were thoroughly evaluated in their entirety, with only those presenting concrete operational frameworks being included in the final review. Finally, data extraction and analysis were carried out on these 82 included articles. The extracted data comprehensively covered key dimensions such as technology type, target infrastructure, specific frameworks, implementation methods, limitations, and associated challenges, providing a robust foundation for the subsequent synthesis and analysis. The PRISMA flow diagram (Fig 2 and Table1) provides a transparent overview of the selection process and ensures replicability.

Table 1. Methodology Summary Table

Stage	# Articles	Description
Identification	350	Articles retrieved from IEEE, ScienceDirect, SpringerLink, Scopus
Duplicates removed	120	Duplicate or similar versions excluded
Remaining after duplicates	230	Articles remaining after duplicate removal
Title and abstract screening	148 excluded	Irrelevant or purely theoretical articles removed
Full-text assessment / Included	82	Articles with operational frameworks selected
Data extraction & analysis	82	Extracted: technology type, target infrastructure, frameworks, implementation methods, limitations, and challenges

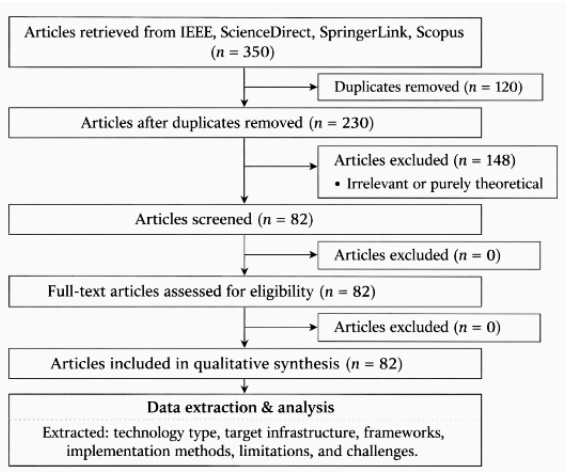


Fig 2. PRISMA Flow Diagram of the Methodology

Extracted data included:

Following data collection, a comprehensive comparative analysis and categorization of the identified frameworks were conducted. This process focused on integrated technologies specifically AI, Blockchain, and IoT applied to target infrastructures such as Industry 5.0 and Smart Cities. The evaluation centered on proposed frameworks or models, implementation and performance evaluation methods, as well as operational challenges and limitations. By assessing these elements based on scalability, security, sustainability, and feasibility, the study aimed to systematically identify research gaps and uncover practical innovation opportunities.

2.5 Research Limitations

Despite the rigorous methodological approach adopted in this study, several inherent limitations must be acknowledged to provide a balanced perspective on the findings. First, regarding database coverage, the review was confined to major international academic databases; consequently, relevant studies published in local journals, conference proceedings, or less-accessible repositories may have been inadvertently overlooked, potentially narrowing the scope of the evidence base. Second, a language restriction was applied, limiting the inclusion to articles published exclusively in English. While this facilitates a standardized analysis, it introduces a potential language bias by excluding valuable insights from non-English speaking regions, which might offer different contextual perspectives on technology implementation. Third, publication bias remains a concern, as the academic literature tends to favor the dissemination of studies reporting successful implementations or positive outcomes. This skew may result in an underrepresentation of negative results, failed attempts, or inconclusive findings, thereby presenting an overly optimistic view of the current state of the field. Finally, the rapid pace of technological evolution in the domains of AI, Blockchain, and IoT poses a dynamic challenge. Given the speed at which these technologies advance, some of the frameworks and methodologies discussed in the selected articles may already be becoming obsolete or require significant updates shortly after their publication, highlighting the need for continuous monitoring and updating of such reviews to remain relevant.

3 Overview of Key Technologies

This section presents a comprehensive examination of the three pivotal technologies under investigation: Artificial Intelligence (AI), Blockchain, and the Internet of Things (IoT). It critically analyzes their specific applications, inherent benefits, and associated challenges within the contexts of Industry 5.0 and smart city infrastructures. The primary objective is to elucidate the distinct role of each technology and explore their convergence potential, thereby laying the groundwork for the design of robust, integrated frameworks.

Artificial Intelligence serves as the cognitive core of these systems, leveraging machine learning algorithms and natural language processing to analyze vast datasets generated by sensors. This capability enables autonomous decision-making and predictive analytics, transforming raw data into actionable insights. Conversely, the Internet of Things functions as the sensory and execution layer, establishing physical connectivity between devices to facilitate real-time data collection and transmission. Blockchain complements these technologies by providing a decentralized, immutable, and transparent distributed ledger, which ensures security, traceability, and trust in transactions and interactions among devices or stakeholders.

In the realm of Industry 5.0, the synergy of these technologies extends beyond mere automation; it fosters human-machine collaboration that is both intelligent and sustainable. For instance, in a smart factory, IoT sensors continuously monitor equipment status, AI predicts potential failures through pattern recognition, and Blockchain securely records maintenance histories and supply chain transactions. Similarly, in smart cities, this technological convergence optimizes traffic management, enables intelligent energy distribution, and enhances the security and efficiency of urban services. However, the implementation of such integrated frameworks is not without obstacles. Significant challenges include technical complexity, the necessity for robust communication infrastructure, privacy concerns, and the lack of standardized protocols. Ultimately, this section aims to provide a deep understanding of how these technologies interact and complement one another, facilitating the development of practical frameworks that maximize their collective advantages while mitigating individual limitations.

3.1 Artificial Intelligence in Industry 5.0 and Smart Cities

Artificial Intelligence (AI) functions as the cognitive engine driving intelligent analysis and autonomous decision-making within the ecosystems of Industry 5.0 and smart cities [13]. Unlike the rigid automation of previous industrial paradigms, AI in this context emphasizes adaptability, human-centricity, and sustainability. Its applications are multifaceted, spanning from granular industrial processes to complex urban management systems.

Firstly, in the realm of industrial and urban data analytics, AI algorithms process massive volumes of heterogeneous data to optimize critical resources. In Industry 5.0, this involves analyzing production line metrics in real-time to minimize waste and energy consumption, thereby supporting sustainable manufacturing goals. Similarly, in smart cities, AI analyzes data streams from utility grids to balance energy loads efficiently, predicting peak demands and adjusting distribution dynamically to reduce carbon footprints. This capability extends to resource management, where AI models simulate various scenarios to determine the most efficient allocation of water, electricity, and raw materials, ensuring both economic viability and environmental stewardship.

Secondly, AI enables sophisticated automated decision-making and predictive capabilities through advanced machine learning (ML) and deep learning (DL) techniques. In industrial settings, predictive maintenance algorithms analyze vibration, temperature, and acoustic data from machinery to forecast potential failures before they occur, significantly reducing downtime and maintenance costs. In urban environments, these algorithms are pivotal for traffic management and demand forecasting. For instance, AI-driven traffic lights adjust signal timings based on real-time vehicle flow, reducing congestion and emissions. Furthermore, in public services, AI predicts demand for transportation and utilities, allowing city planners and operators to allocate resources proactively rather than reactively.

Thirdly, AI plays a crucial role in smart urban service management by optimizing essential services such as transportation, public lighting, and waste management. Intelligent algorithms can control street lighting systems to dim or brighten based on pedestrian and vehicle presence, saving energy while maintaining safety. In waste management, AI optimizes collection routes by analyzing fill-levels of smart bins, reducing fuel consumption and operational costs. These applications demonstrate how AI transforms static urban infrastructure into responsive, adaptive systems that improve quality of life for citizens.

Regarding practical implementation, several studies propose multi-layered architectural frameworks to structure AI integration effectively [14]. These architectures typically consist of three distinct layers: the perception layer, responsible for data collection via IoT sensors; the processing layer, where data is cleaned, aggregated, and analyzed using AI models; and the application layer, which executes intelligent decisions and provides user interfaces for stakeholders. This layered approach ensures modularity and scalability, allowing cities and industries to upgrade specific components without overhauling the entire system.

However, the deployment of AI in these contexts is accompanied by significant challenges and limitations. One primary hurdle is the sheer volume and velocity of data, which require real-time processing capabilities that can strain existing computational infrastructure. Handling big data streams necessitates robust edge computing solutions to reduce latency and bandwidth usage. Secondly, the effectiveness of AI models is heavily dependent on data quality; incomplete, noisy, or biased data can lead to inaccurate predictions and flawed decisions. The lack of standardized data formats across different devices and platforms exacerbates this issue, making data integration and interoperability difficult [7,10,14]. Finally, integrating AI with other emerging technologies like IoT and Blockchain adds layers of complexity. Ensuring seamless communication between AI decision engines, IoT data sources, and Blockchain security protocols requires sophisticated middleware and standardized protocols, which are still evolving. Addressing these technical and organizational barriers is essential for realizing the full potential of AI in Industry 5.0 and smart city initiatives [1,13].

3.2 Blockchain in Industrial and Urban Infrastructures

Blockchain technology emerges as a foundational pillar for establishing security, trust, and data transparency within the complex ecosystems of Industry 5.0 and smart cities. By providing a decentralized and immutable ledger, blockchain addresses critical vulnerabilities associated with centralized data management, ensuring that information exchanged between diverse stakeholders remains authentic and tamper-proof. Its applications are deeply integrated into the operational fabric of modern industrial and urban environments, primarily focusing on three key areas: data integrity, process automation, and supply chain visibility [15].

Firstly, blockchain ensures data integrity and authenticity, which is particularly crucial when dealing with the vast streams of information generated by Internet of Things (IoT) sensors. In smart factories and urban monitoring systems, sensors collect real-time data regarding equipment status, environmental conditions, and resource usage. Without blockchain, this data is vulnerable to manipulation or corruption during transmission or storage. Blockchain mitigates these risks by cryptographically linking each data entry to the previous one, creating a verifiable chain of custody. This ensures that any decision made based on sensor data such as adjusting a robotic arm or altering traffic light signals is grounded in accurate, unaltered information, thereby enhancing the reliability of automated systems.

Secondly, the implementation of smart contracts revolutionizes industrial and urban processes by enabling self-executing agreements that operate without intermediaries. Smart contracts are digital protocols that automatically enforce and execute the terms of an agreement when predefined conditions are met. In Industry 5.0, this can streamline procurement processes, where payments are automatically released to suppliers upon the verified delivery of goods. In smart cities, smart contracts can manage energy trading between prosumers (consumers who also produce energy, such as those with solar panels), allowing peer-to-peer energy exchanges to occur seamlessly and securely. This automation reduces administrative overhead, minimizes human error, and accelerates transaction speeds, fostering a more efficient and responsive infrastructure.

Thirdly, blockchain plays a pivotal role in supply chain traceability and management, ensuring the authenticity and tracking of goods and resources from origin to consumption. In complex global supply chains, maintaining visibility into the provenance of raw materials and finished products is essential for quality control, regulatory compliance, and ethical sourcing. Blockchain provides an end-to-end transparent record of every transaction and movement within the supply chain. For instance, in the pharmaceutical industry, blockchain can track drugs from manufacturing to pharmacy, preventing counterfeit products from entering the market. Similarly, in smart city waste management, it can track the disposal and recycling of materials, ensuring compliance with environmental regulations and promoting circular economy practices.

Regarding practical implementation, private and hybrid blockchain networks are commonly proposed for managing industrial and urban data [16]. Unlike public blockchains, which are open to anyone and may suffer from scalability issues, private blockchains restrict access to authorized participants, offering greater control over data privacy and transaction speed. Hybrid blockchains combine the benefits of both public and private networks, allowing sensitive data to remain within a private network while using a public ledger for verification and transparency. This flexibility makes them suitable for diverse applications, from secure industrial communication to transparent public service delivery [88,90,91].

The nascent integration of blockchain technology into the construction sector, particularly for enhancing information management, has garnered significant scholarly attention. Recent research has demonstrated its applicability across various phases of construction projects, addressing long-standing challenges of data transparency, traceability, and trust. For instance, Wu et al. (2022a) investigated the use of blockchain to improve the accuracy of information sharing specifically during the critical onsite assembly phase of modular construction, highlighting its potential to mitigate errors and delays [88]. Expanding on the modular construction theme, the same research group explored the integration of a permissioned blockchain with an IoT-BIM platform to manage the off-site production chain, creating an auditable and trustworthy digital thread for prefabricated components [89]. Beyond specific applications, studies have also begun to address the foundational technical considerations for implementation. Xu et al. (2023) provided a critical analysis of various consensus protocols, evaluating their suitability for the unique requirements and constraints of blockchain-based applications within the construction industry [90]. Furthermore, the strategic choice between different blockchain architectures has been examined. Yang et al. (2020) analyzed the comparative roles of public and private blockchains, discussing their implications for business process and information integration in construction contexts [91]. This body of work collectively establishes blockchain as a promising technological enabler for digital transformation in construction, focusing on data integrity, process efficiency, and secure collaboration across fragmented project teams.

However, the adoption of blockchain in these infrastructures is not without significant challenges and limitations. One major concern is the high energy consumption associated with certain consensus algorithms, particularly Proof of Work (PoW). As industrial and urban systems scale up, the computational power required to validate transactions can lead to substantial energy costs and environmental impacts, contradicting the sustainability goals of Industry 5.0 and smart cities. Consequently, there is a growing shift towards more energy-efficient consensus mechanisms like Proof of Stake (PoS) or Byzantine Fault Tolerance (BFT).

Furthermore, the implementation complexity at a large scale poses a significant barrier. Integrating blockchain with existing legacy systems, IoT devices, and AI platforms requires sophisticated middleware and robust architectural design. The heterogeneity of devices and protocols in industrial and urban settings complicates the standardization of data formats and communication interfaces, making seamless integration challenging. Additionally, the need for standardization and interoperability with other technologies remains a critical issue. Without common standards, different blockchain platforms may operate in silos, limiting their ability to communicate and share data effectively [8,15,16,62]. Establishing universal protocols for blockchain interoperability is essential to create a cohesive and interconnected ecosystem where AI, IoT, and blockchain can work together harmoniously to drive innovation and efficiency in Industry 5.0 and smart cities.

3.3 Internet of Things and Smart Data Collection

The Internet of Things (IoT) serves as the foundational sensory layer that enables real-time data collection infrastructure by seamlessly connecting physical devices, sensors, and actuators across industrial and urban environments [17]. By bridging the gap between the physical and digital worlds, IoT transforms static assets into intelligent nodes capable of generating, transmitting, and responding to data streams. This connectivity is critical for creating responsive ecosystems in Industry 5.0 and smart cities, where immediate awareness of environmental and operational conditions drives efficiency and sustainability.

In practical terms, the application of IoT spans a wide array of industrial and urban sensors designed to capture granular data. In industrial settings, sensors monitor critical parameters such as temperature, pressure, vibration, and humidity to ensure optimal production conditions and worker safety. In urban contexts, these sensors track environmental quality (e.g., air pollution levels), traffic flow dynamics, and energy consumption patterns across buildings and streetlights. This continuous data generation provides a comprehensive view of system performance, allowing stakeholders to move from reactive maintenance to proactive management. For instance, smart meters in a city grid can detect fluctuations in energy demand instantly, enabling utilities to balance loads and prevent outages before they occur.

Furthermore, IoT facilitates smart monitoring and control, allowing for the real-time management of equipment and urban services. Through connected devices, operators can remotely monitor the status of machinery or infrastructure and execute control commands instantly. In a smart factory, this might involve adjusting robotic arms based on real-time quality control data. In smart cities, it could mean dynamically adjusting traffic signals to alleviate congestion or regulating street lighting based on pedestrian presence. This level of control enhances operational efficiency, reduces waste, and improves the quality of life for citizens by ensuring that services are delivered precisely when and where they are needed.

A crucial aspect of IoT's value proposition lies in its integration with Artificial Intelligence (AI) and Blockchain. IoT devices generate massive volumes of raw data, which, without processing, holds limited value. By integrating with AI, IoT data can be analyzed to extract meaningful insights, predict trends, and automate decision-making processes. Simultaneously, integrating with Blockchain ensures the security and integrity of this data stream. This triad creates a robust ecosystem where IoT provides the data, AI provides the intelligence, and Blockchain provides the trust and security, collectively enabling reliable and processed data for intelligent decision-making.

Regarding practical implementation, typical IoT architectures are structured into three distinct layers: the perception layer, the network layer, and the processing layer [18,45]. The perception layer consists of sensors and actuators that collect physical data. The network layer handles the transmission of this data via various communication protocols (e.g., Wi-Fi, Zigbee, 5G, LoRaWAN). The processing layer, often involving cloud or edge computing, is where data is stored, analyzed, and acted upon. Edge computing, in particular, has gained prominence as it allows data processing to occur closer to the source, reducing latency and bandwidth usage, which is essential for time-sensitive applications like autonomous vehicles or industrial robotics.

However, the widespread adoption of IoT faces significant challenges and limitations. First and foremost is the issue of security and privacy. With billions of connected devices, the attack surface for cyber threats expands dramatically. IoT devices often have limited computational power, making it difficult to implement robust security measures, leaving them vulnerable to hacking and data breaches. Ensuring the privacy of sensitive data collected from homes, workplaces, and public spaces is also a major concern, requiring strict data governance and encryption standards.

Secondly, energy consumption and resource management at a large scale pose a significant hurdle. Many IoT devices are battery-powered and deployed in hard-to-reach locations, making frequent battery replacement impractical. Therefore, developing energy-efficient sensors and communication protocols is crucial. Additionally, the sheer volume of data generated by IoT networks can overwhelm existing infrastructure, necessitating advanced data compression and management techniques [17,18,52,45,83].

Finally, the need for communication standards and interoperability among devices remains a critical barrier. The IoT landscape is fragmented, with numerous proprietary protocols and platforms that often do not communicate with each other effectively. This lack of standardization leads to siloed systems, hindering seamless integration and data exchange. Establishing universal standards for connectivity and data formats is essential to create a cohesive IoT ecosystem where devices from different manufacturers can work together harmoniously, maximizing the potential of Industry 5.0 and smart city initiatives.

3.4 Convergence of Technologies and Practical Frameworks

The true transformative potential of Industry 5.0 and smart city infrastructures is not realized through the isolated deployment of Artificial Intelligence (AI), Blockchain, or the Internet of Things (IoT), but rather through their deep, synergistic convergence. This integration creates a holistic ecosystem where scalability, security, and intelligence are mutually reinforcing [10,12]. While each technology offers distinct advantages IoT for sensing, Blockchain for trust, and AI for cognition their combined architecture addresses the limitations of individual systems, enabling robust, autonomous, and transparent operations. Practical frameworks for this convergence typically follow a tri-layered model: the Data Collection Layer, the Security and Trust Layer, and the Processing and Decision-Making Layer. However, the path to realizing this vision is fraught with significant technical, operational, and critical challenges that require nuanced analysis beyond theoretical benefits.

1.The Data Collection Layer: IoT as the Sensory Foundation

At the base of the convergence framework lies the IoT layer, which serves as the extensive sensory network of the system. This layer comprises billions of heterogeneous devices, sensors, and actuators deployed across industrial plants and urban landscapes. These devices are responsible for capturing real-time physical data, such as temperature, pressure, location, motion, and environmental conditions. In a practical scenario, such as a smart manufacturing plant, IoT sensors monitor the vibration and heat of robotic arms, while in a smart city, they track air quality and traffic density.

However, the sheer scale and heterogeneity of this layer present immediate challenges. The diversity of hardware manufacturers and communication protocols (e.g., Zigbee, LoRaWAN, NB-IoT, 5G) often leads to fragmentation. Data collected from these devices is frequently unstructured, noisy, and incomplete. Without rigorous preprocessing at the edge, this raw data can overwhelm downstream systems. Furthermore, the energy constraints of battery-powered IoT devices limit their operational lifespan, necessitating energy-harvesting technologies or low-power wide-area network (LPWAN) solutions. The critical issue here is not just data collection, but the reliable and continuous transmission of high-fidelity data, which forms the bedrock for all subsequent intelligent processes.

2 .The Security and Trust Layer: Blockchain as the Immutable Ledger

Above the data collection layer sits the Blockchain layer, which acts as the backbone of trust and security. In a decentralized environment where data flows from numerous IoT devices to various stakeholders, ensuring data integrity and authenticity is paramount. Blockchain provides a distributed, immutable ledger that records every transaction and data exchange. This layer ensures that data collected by IoT sensors has not been tampered with during transmission or storage.

For instance, in a supply chain management system, IoT sensors track the temperature of pharmaceutical products during transit. This data is hashed and recorded on a blockchain. If a temperature deviation occurs, the blockchain provides an unalterable record of the event, ensuring accountability. Smart contracts, which are self-executing contracts with the terms of the agreement directly written into code, operate within this layer. They automate processes based on predefined conditions, such as releasing payment only when IoT-verified delivery conditions are met. This eliminates the need for intermediaries, reduces administrative costs, and minimizes the risk of fraud.

However, the integration of Blockchain introduces significant overhead. The consensus mechanisms required to validate transactions consume substantial computational resources and energy, particularly in Proof-of-Work (PoW) systems. While Proof-of-Stake (PoS) and other energy-efficient consensus algorithms are being adopted, the latency associated with blockchain validation can conflict with the real-time requirements of IoT applications. Additionally, the immutability of blockchain poses a challenge regarding data privacy and the "right to be forgotten," as mandated by regulations like GDPR. Storing personal or sensitive data directly on a public blockchain is often non-compliant, necessitating complex hybrid architectures where only hashes or metadata are stored on-chain, while the actual data remains off-chain in secure databases.

3 .The Processing and Decision-Making Layer: AI as the Cognitive Engine

The apex of the convergence framework is the AI layer, which processes the verified data from the IoT layer, secured by the Blockchain layer, to generate actionable insights and automate decisions. AI algorithms, including machine learning (ML) and deep learning (DL), analyze vast datasets to identify patterns, predict future trends, and optimize operations. In Industry 5.0, AI enables predictive maintenance by analyzing sensor data to forecast equipment failures before they occur, thereby reducing downtime and maintenance costs. In smart cities, AI optimizes traffic flow by analyzing real-time data from cameras and sensors, adjusting signal timings to minimize congestion and emissions.

The synergy between AI and Blockchain is particularly powerful. Blockchain ensures the quality and provenance of the data used to train AI models, mitigating the risk of biased or corrupted data. Conversely, AI can optimize blockchain operations by predicting network congestion and adjusting consensus parameters dynamically. For example, AI can analyze transaction patterns to predict peak loads on the blockchain network and adjust resource allocation accordingly [19,22,27].

Despite these benefits, the AI layer faces challenges related to interpretability and computational intensity. Complex deep learning models often operate as "black boxes," making it difficult for stakeholders to understand the rationale behind specific decisions. In critical applications like healthcare or autonomous driving, this lack of transparency can hinder trust and adoption. Furthermore, the computational requirements for training and running large AI models are substantial, often requiring cloud-based infrastructure that may introduce latency. Edge AI, which performs computations closer to the data source, is emerging as a solution, but it requires powerful, energy-efficient edge devices that are currently costly and complex to deploy at scale [10,12,19,21,22,27]. Fig 3 shows the integration of these technologies in the industry.

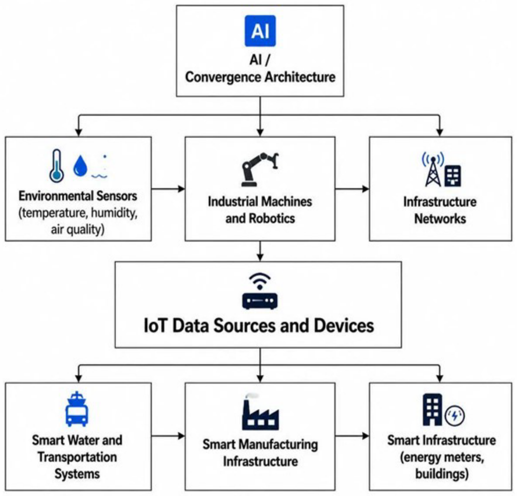


Fig 3. Convergence Framework of AI, Blockchain, and IoT

Critical Analysis and Operational Challenges

While the theoretical framework for the convergence of AI, Blockchain, and IoT is compelling, its practical implementation is hindered by several critical operational challenges.

Interoperability and Standardization: One of the most significant barriers is the lack of universal standards for interoperability. IoT devices, blockchain platforms, and AI frameworks often operate in silos, using different data formats, communication protocols, and APIs. This fragmentation makes it difficult to create seamless, integrated systems. For example, an IoT sensor from Manufacturer A may not easily communicate with a blockchain platform from Provider B, which in turn may not be compatible with the AI model from Vendor C. Developing and adopting open standards is essential to enable cross-platform compatibility and data exchange. Initiatives like the Industrial Internet Consortium (IIC) and the Open Connectivity Foundation (OCF) are working towards this goal, but widespread adoption remains slow.

Energy Consumption and Sustainability: The convergence of these technologies raises serious concerns about energy consumption and environmental impact. IoT devices, blockchain networks, and AI models all require significant energy resources. The cumulative energy footprint of billions of connected devices, continuous blockchain transactions, and large-scale AI computations can be substantial. This contradicts the sustainability goals of Industry 5.0 and smart cities, which aim to reduce carbon emissions and promote green practices. There is a critical need for energy-efficient algorithms, hardware, and protocols. For instance, developing lightweight blockchain consensus mechanisms and energy-efficient AI models is crucial. Additionally, leveraging renewable energy sources to power IoT infrastructure and data centers can help mitigate the environmental impact.

Security and Privacy: While Blockchain enhances security, the convergence of AI, IoT, and Blockchain also introduces new attack vectors. IoT devices are often vulnerable to hacking, which can compromise the entire system. If an attacker gains control of IoT sensors, they can feed false data to the blockchain, corrupting the ledger and misleading AI algorithms. This "garbage in, garbage out" problem can lead to catastrophic failures in critical systems. Furthermore, the integration of AI with blockchain raises privacy concerns. While blockchain ensures data integrity, it does not inherently protect privacy. AI algorithms can potentially infer sensitive information from seemingly innocuous data points, leading to privacy breaches. Developing robust security measures, including encryption, access control, and anomaly detection, is essential to protect the converged system from cyber threats.

Scalability and Performance: As the number of connected devices and transactions increases, the scalability of the converged system becomes a major challenge. Blockchain networks, in particular, face scalability issues due to the need for consensus among all nodes. As the network grows, the time required to validate transactions increases, leading to bottlenecks and high latency. This is particularly problematic for real-time applications like autonomous driving or industrial automation, where milliseconds matter. Solutions like sharding, sidechains, and layer-2 scaling solutions are being explored, but they add complexity to the system architecture. Similarly, AI models require significant computational resources to process large datasets in real-time, which can strain edge devices and cloud infrastructure [19,22,27,87,89].

Case Study: Smart Grid Energy Trading

To illustrate the practical convergence and its challenges, consider a smart grid energy trading platform. In this system, IoT smart meters collect real-time energy consumption and production data from households and businesses. This data is hashed and recorded on a blockchain, ensuring transparency and immutability. Smart contracts automatically facilitate peer-to-peer energy trading, allowing prosumers (consumers who also produce energy, e.g., via solar panels) to sell excess energy to neighbors. AI algorithms analyze historical and real-time data to predict energy demand and supply, optimizing pricing and grid stability [18].

However, this system faces several challenges. The high frequency of transactions required for real-time energy trading can overwhelm the blockchain network, leading to high latency and transaction fees. The heterogeneity of smart meters from different manufacturers can lead to interoperability issues, making it difficult to standardize data formats. The computational intensity of AI models for demand prediction can strain edge devices, requiring cloud offloading, which introduces latency and privacy concerns. Furthermore, the energy consumption of the blockchain network and AI computations must be carefully managed to ensure the system remains sustainable [19,70,75].

The convergence of AI, Blockchain, and IoT offers a powerful framework for building scalable, secure, and intelligent systems in Industry 5.0 and smart cities. By integrating data collection, security, and intelligence, this convergence enables autonomous decision-making, enhanced transparency, and improved efficiency. However, realizing this potential requires addressing significant challenges related to interoperability, energy consumption, security, privacy, and scalability. Overcoming these obstacles will require collaborative efforts from industry stakeholders, researchers, and policymakers to develop open standards, energy-efficient technologies, and robust security measures. Only through a holistic and critical approach can the true promise of this technological convergence be fully realized, leading to more sustainable, efficient, and human-centric industrial and urban environments [1,18,70].

4 Frameworks for AI–Blockchain–IoT Convergence

This section reviews frameworks and practical models for the convergence of Artificial Intelligence (AI), Blockchain, and the Internet of Things (IoT) in developing Industry 5.0 and smart city infrastructures**.** The aim is to identify technical architectures, implementation models, and the strengths and weaknesses of each framework to provide practical and operational insights [20].

4.1 Technical Architectures for Convergence

Convergent architectures generally include three main layers**:**

1. Data Collection Layer (IoT Layer):
- IoT sensors and devices collect environmental, industrial, and urban data [21].
- Data is transmitted to the processing layer in real-time or periodically.
- Example: energy consumption sensors in smart buildings or industrial machine sensors [22].
2. Security and Trust Layer (Blockchain Layer):
- Collected data is recorded and encrypted on the blockchain to ensure integrity and transparency [23].
- Smart contracts automate industrial and urban processes [24].
- Proposed models include private, hybrid, or combined public-private blockchain networks [25].
3. Processing and Decision-Making Layer (AI Layer):
- AI algorithms analyze and predict based on the collected data [26].
- Intelligent decisions optimize production, energy consumption, traffic, and urban services [21].
- Integration with blockchain and IoT data enhances decision accuracy and security [24].

4.2 Practical Models and Use Cases

Several studies and pilot projects have proposed the following models:

1. Edge AI and Blockchain Framework: IoT data is processed at the network edge and then sent to the blockchain, ensuring low latency and data security [26].
2. Cloud AI and Hybrid Blockchain Framework: Data is first sent to cloud servers, AI processing is performed, and results are recorded on the blockchain [23].
3. IoT–AI–Blockchain Framework for Urban Management: Optimizes transportation, lighting, energy consumption, and waste management using collected data, AI analytics, and secure blockchain recording [25].

4.3 Challenges and Practical Limitations

Despite the benefits of convergence, frameworks face the following challenges:

1. Energy and resource consumption: AI algorithms and blockchain consensus mechanisms are computationally intensive [24].
2. Interoperability and standardization: Devices and systems must adhere to common protocols and standards for effective integration [25].
3. Scalability: Increasing numbers of sensors and data volume can reduce system performance [26].
4. Implementation complexity: Designing and deploying operational frameworks requires multidisciplinary expertise in AI, Blockchain, and IoT [20].

4.4 Innovation Opportunities

Identified challenges also present opportunities for innovation in convergent frameworks:

1. Optimizing AI and blockchain consensus algorithms to reduce energy consumption [24]
2. Developing common standards and protocols to improve system interoperability [25]
3. Using hybrid edge and cloud computing for enhanced scalability and low-latency response [26]
4. Implementing pilot and test systems in industrial and urban environments before large-scale deployment [23]

5 Analysis, Comparative Review, and Discussion of Systematic Review Findings

This section provides a detailed analysis of 82 selected articles from the systematic review, focusing on innovation, scientific value, and the originality of frameworks**.** The aim is to offer practical comparisons, critical analysis, and identification of research gaps and opportunities**.**

5.1 Technologies and Innovations

Analytical Overview: Artificial Intelligence (AI), Blockchain, and the Internet of Things (IoT) are the three key technologies applied in Industry 5.0 and smart cities. AI enables intelligent decision-making and real-time prediction, with recent innovations including deep learning algorithms integrated with edge computing [27, 28]. Blockchain contributes to data security, transparency, and smart contract execution, where hybrid networks and multi-step smart contracts provide practical and security innovations [29, 30]. IoT allows real-time data collection and intelligent device control, and its integration with edge computing represents a critical practical innovation [30, 31] (Table2).

5.2 AI–Blockchain–IoT Convergence Frameworks

Analytical Overview: Practical convergence frameworks typically consist of three layers: Data Collection (IoT), Security and Trust (Blockchain), and Processing & Decision-Making (AI). Edge AI reduces latency and enhances data security, while Cloud AI combined with Hybrid Blockchain provides scalability and advanced analytics [28], [30], [31]. Urban frameworks integrating these technologies enable optimized energy consumption and smart service management [32] (Table3).

Table 2. Analysis of Key Technologies with Innovation Perspective

Technology	Main Application	Innovation	Advantages	Limitations	Reference
AI	Data analysis, intelligent decision-making	Deep learning algorithms with real-time processing	Improved efficiency, error reduction	High-quality data requirement, heavy computation	[27], [28]
Blockchain	Data security, smart contracts	Hybrid networks, multi-step contracts	Trust, transparency, fraud reduction	High energy consumption, implementation complexity	[29], [30]
IoT	Real-time data collection, monitoring	Smart sensors and edge computing	Accurate and timely data, real-time control	Security and privacy concerns, energy consumption	[30], [31]

Table 3. Practical AI–Blockchain–IoT Convergence Frameworks

Framework	Layers	Implementation Example	Performance Indicators	Innovation	Advantages	Limitations	Reference
Edge AI + Blockchain	IoT + AI + Blockchain	Smart factory, energy network	Low latency, data security	Edge processing, fast blockchain recording	Fast response, high security	Implementation complexity, energy consumption	[31], [28]
Cloud AI + Hybrid Blockchain	IoT + AI + Blockchain	Urban management, smart transportation	Prediction accuracy, data security	Combination of cloud processing and smart contracts	Scalability, advanced analytics	Network dependency, cloud resource consumption	[30], [28]
Urban IoT–AI–Blockchain	IoT + AI + Blockchain	Energy optimization, waste, traffic management	Urban efficiency, error reduction	Multi-layer technology integration	Automation, intelligent decision-making	Standardization, scalability, security	[32], [29]

Table 4. Research Gaps, Critical Points, and Innovation Opportunities

Gap / Critical Point	Description	Innovation Opportunity	Reference
Standardization	Lack of common protocols for technology interoperability	Development of modular standards and APIs	[32], [30]
Energy Consumption	Heavy processing and blockchain consensus	Optimized algorithms and edge computing	[31], [33]
Real-World Evaluation	Limited practical data	Industrial and urban pilot projects	[28], [29]
Multi-Technology Integration	Tested mostly in simulation	Real-world and large-scale testing	[27], [33]
Innovation	Edge AI, multi-step smart contracts	Development of practical and deployable frameworks	[27], [30], [32],[35],[51],[52],[84],[85]

5.3 Research Gaps and Innovation Opportunities

Analytical Overview: Critical analysis reveals that standardization, energy consumption, real-world evaluation, and multi-technology integration remain key limitations [27], [31], [32],[35],[51],[52] (Table4). However, Edge AI, hybrid networks, and multi-step smart contracts provide significant practical and scientific value and innovation.

5.4 Comparative Review of Existing Studies and Research Gap

The convergence of Artificial Intelligence (AI), Blockchain, and the Internet of Things (IoT) has recently emerged as a fundamental research direction for enabling Industry 5.0 and Smart City infrastructures. However, existing studies have largely investigated these technologies in isolation or in partial combinations, resulting in fragmented knowledge and the absence of implementation-oriented convergence frameworks.

This section presents a critical and integrated review of thirty representative and highly cited studies to identify existing research gaps and position the novelty of the present work.
Early research primarily focused on the integration of Blockchain and IoT to address security and trust challenges in smart environments. Atzori [50] introduced one of the earliest visions of the Blockchain-of-Things paradigm, demonstrating how distributed ledgers can mitigate security vulnerabilities in IoT networks. Similarly, Dai et al. [51] highlighted the importance of decentralized trust management in IoT ecosystems, arguing that blockchain can significantly improve data integrity and device authentication. Subsequent survey studies further reinforced this perspective, showing that blockchain enables transparency, trust, and secure data sharing in smart city infrastructures [52] – [54]. While these studies established the importance of blockchain in IoT ecosystems, they did not incorporate AI-driven analytics or Industry 5.0 perspectives.
Parallel to blockchain research, another body of literature focused on AI and IoT integration for Industry 4.0. Lee et al. [55] emphasized the role of AI and big data analytics in smart manufacturing, demonstrating how predictive analytics can optimize industrial processes. Zonta et al. [56] expanded this concept by presenting AI-driven predictive maintenance models using IoT data. Similarly, Xu et al. [57] and Leng et al. [58] highlighted the importance of digital twins and intelligent automation in Industry 4.0 environments. Although these studies significantly advanced AI-IoT integration, they largely ignored decentralized trust, governance, and security mechanisms, which are essential for large-scale deployment in smart cities.
The concept of Industry 5.0 introduced a new research direction emphasizing human-centric automation and sustainability. Nahavandi [59] defined Industry 5.0 as the next stage of industrial transformation, focusing on collaboration between humans and intelligent machines. Later studies confirmed that AI and IoT play a central role in enabling human-machine collaboration and real-time decision-making, Cyber-physical systems (CSP) in smart manufacturing [60], [61]. Nevertheless, the role of blockchain in enabling secure collaboration and data sharing in Industry 5.0 remains insufficiently explored.
Recent research has begun to explore the simultaneous integration of AI, Blockchain, and IoT. For example, several studies demonstrated that combining the three technologies can significantly enhance cybersecurity, privacy, and operational efficiency in smart cities [62]–[65]. Edge computing and 6G-enabled architectures further strengthened this convergence by enabling decentralized intelligence and ultra-low latency communication [66], [67]. Notably,[67] proposed a foundational framework integrating AI and blockchain to ensure trust and security, while treating IoT as a peripheral component, though it faced challenges related to scalability and energy consumption. In addition, emerging research has applied the tri-technology paradigm to specific domains such as smart healthcare, smart transportation, smart grids, and supply chains [68]–[73]. Despite these advancements, most studies remain domain-specific and do not provide generalizable architectural frameworks.
Another important research direction involves federated learning and edge AI for privacy-preserving analytics in IoT environments [74], [75], [79]. These approaches reduce data sharing risks but still lack decentralized trust and governance mechanisms, which blockchain can provide. Similarly, blockchain-based energy trading and supply chain management studies highlight the importance of decentralized infrastructures but do not integrate advanced AI analytics [76]–[78]. a comparative analysis of selected key studies is presented in Table 5. This synthesis highlights the technologies employed, primary focus or use cases, key contributions, and identified limitations of each study. The table incorporates seminal works previously discussed in the literature review
Overall, the literature clearly confirms the importance of AI, Blockchain, and IoT convergence. However, the following critical gaps remain:

1. Lack of unified multi-layer architectures integrating all three technologies
2. Limited focus on simultaneous Industry 5.0 and Smart City applications
3. Absence of implementation-oriented design criteria
4. Insufficient analysis of interoperability, scalability, and energy efficiency

Therefore, the present study addresses these gaps by providing a systematic and practical review of deployable convergence frameworks that integrate AI at the analytics layer, blockchain at the trust and governance layer, and IoT at the sensing and data acquisition layer.

6 Roadmap for Future Research and Implementation

The convergence of three foundational technologies Artificial Intelligence (AI), Blockchain (BC), and the Internet of Things (IoT) is recognized as the core of digital transformation toward Industry 5.0 and next-generation smart cities. This integration enhances security, autonomy, flexibility, and intelligence across infrastructural systems. Achieving this vision requires a structured, phased, and time-bound roadmap [48,80-87]. See Table 6 for detailed phase and timelines.

Phase 1 — 2025–2026: Establishment of Data Foundations and IoT Infrastructure

- Deployment of 5G/6G communication networks
- Installation of IoT sensors across industrial, transportation, energy, and environmental sectors
- Development of multi-source data repositories
- Design of preliminary AI–IoT communication architectures
- Formulation of initial cybersecurity and privacy frameworks

Table 5. Comparison of Previous Studies and Novelty of This Research

Ref	Main Focus	AI Role	Blockchain Role	IoT Role	Application Domain	Key Limitation	Contribution Compared to This Study
[50]	Blockchain-of-Things vision	None	Security	IoT core	IoT networks	No AI layer	Adds AI analytics
[51]	Blockchain IoT architecture	Limited	Trust	Sensors	IoT ecosystems	No Industry 5.0	Adds Industry 5.0 perspective
[52]	Blockchain Smart Cities survey	None	Governance	Urban IoT	Smart cities	No AI integration	Tri-technology integration
[53]	Blockchain IoT security survey	None	Security	IoT	Smart environments	No analytics	Adds analytics layer
[54]	Blockchain IoT smart city	Limited	Security	Sensors	Urban services	Conceptual only	Implementation framework
[55]	AI Big Data Industry 4.0	Analytics	None	IoT	Industry	No blockchain	Adds trust layer
[56]	AI predictive maintenance	ML	None	IoT	Manufacturing	No blockchain	Secure predictive analytics
[57]	Industry 4.0 survey	AI analytics	None	IoT	Industry	No blockchain	Adds decentralized governance
[58]	Digital Twin Industry	AI	None	IoT	Industry	No blockchain	Secure digital twins
[59]	Industry 5.0 concept	Limited	None	IoT	Industry 5.0	No framework	Provides architecture
[60]	Cyber-physical systems (CSP)in smart manufacturing	AI	None	IoT	Industry 4.0	No blockchain	Secure collaboration layer
[61]	AI IoT smart manufacturing	AI	None	IoT	Industry	No blockchain	Adds blockchain trust
[62]	AI-Blockchain cybersecurity	AI	Security	IoT	Smart cities	No architecture	Provides layered framework
[63]	AI Blockchain IoT survey	AI	Security	IoT	Smart cities	Conceptual	Operational comparison
[64]	AI, IoT, Blockchain	AI	Trust	IoT	Industry & IoT	Limited scope	Cross-domain coverage
[65]	AI Blockchain IoT security	AI	Security	IoT	Smart env.	No Industry 5.0	Industry + city integration
[66]	6G Blockchain IoT	Edge AI	Security	IoT	Future networks	Network focus	Application frameworks
[67]	AI Blockchain integration	Intelligent Automation	Trust & Security	Peripheral component	Smart systems	Scalability	Adds decentralized trust, IoT
[68]	Smart healthcare IoT	AI	None	IoT	Healthcare	No blockchain	Secure healthcare framework
[69]	Smart transport AI	AI	None	IoT	Transport	No blockchain	Trustworthy transport
[70]	Smart grid AI	AI	None	IoT	Energy	No blockchain	Secure smart grids
[71]	Federated learning IoT	AI privacy	None	IoT	Healthcare	No blockchain	Adds blockchain governance
[72]	Edge federated IoT	AI	None	IoT	Edge computing	No blockchain	Adds trust layer
[73]	Supply chain blockchain	None	Trust	IoT	Supply chain	No AI	Adds AI optimization
[74]	Blockchain supply chain	None	Security	IoT	Logistics	No AI	Adds analytics layer
[75]	Blockchain energy trading	None	Trust	Smart meters	Energy	No AI	Adds AI forecasting
[76]	Industrial IoT security	Limited	Security	IoT	Industry	No AI integration	Tri-technology security
[77]	Smart agriculture IoT	AI	None	IoT	Agriculture	No blockchain	Trustworthy agriculture
[78]	Edge computing IoT	AI	None	IoT	Smart cities	No blockchain	Adds decentralized governance
[79]	AI IoT smart city survey	AI	None	IoT	Urban	No blockchain	Full convergence framework

Phase 2 — 2027–2028: Intelligence Development and AI-Driven Decision Systems

- Implementation of machine learning and deep learning algorithms on IoT data
- Development of predictive analytics and fault-detection systems in industry
- Use of AI in energy management, transportation flow optimization, and logistics
- Development of Digital Twin models for cities and industrial units
- Initial use of blockchain for sensor data integrity and transaction recording

Phase 3 — 2029–2030: Full Integration of Blockchain with AI and IoT

- Design of lightweight blockchain architectures compatible with IoT devices
- Implementation of Decentralized Identity (DID) systems for devices and users
- Development of Explainable AI (XAI) models
- Deployment of smart contracts for automated industrial process management
- Creation of AI–Blockchain hybrid security systems

Phase 4 — 2031–2032: Implementation of Human-Centered Industry 5.0

- Development of human–machine collaboration systems (Cobots)
- Deployment of intelligent industrial and social robots
- Implementation of adaptive and self-optimizing manufacturing environments
- Use of blockchain for full supply chain traceability
- Application of AI for personalized product and service design

Phase 5 — 2033–2035: Evolution toward Fully Integrated Smart Cities

- Integration of energy, transportation, healthcare, and urban service networks
- Creation of a Meta-Architecture for AI–BC–IoT smart city ecosystems
- Autonomous management of waste, water, and pollution through AI
- Development of intelligent economic systems, automated payments, and data-driven commerce
- International standardization and transition to self-sustainable cities

Table 6. Research and Implementation Roadmap

Year	Key Focus Area	Activities	Expected Outputs
2025	IoT Infrastructure	5G/6G deployment; installation of basic sensors	Baseline environmental and industrial data collection
2026	Data Integration	Development of data platforms; initial security implementation	Stable and secure data repositories
2027	Intelligent Analytics	ML/DL deployment; predictive systems	Early intelligent industrial systems
2028	Digital Twin Development	Urban/industrial modeling; AI enhancement	Digital urban and industrial platforms
2029	Blockchain Integration	Sensor data on BC; smart contract development	Enhanced trust and data integrity
2030	DID and XAI	Decentralized identity; explainable AI	Transparent and trustworthy systems
2031	Human-Centric Systems	Cobots; advanced automation	Industry 5.0 collaborative environments
2032	Smart Supply Chain	Full blockchain traceability	Reduced fraud; improved quality control
2033	Integrated Smart City	Unified energy, health, and transport networks	Centralized smart city management platform
2034	Smart Economy	Automated transactions; data-driven economy	Digital urban economic ecosystem
2035	Full Sustainability	Self-sustaining, AI-managed city systems	Fully evolved Smart City 5.0

This roadmap outlines a structured, time-phased pathway for achieving the convergence of AI, blockchain, and IoT to support the development of Industry 5.0 and next-generation smart city infrastructures. Successful implementation of these phases will lead to autonomous, secure, resilient, and human-centered technological ecosystems capable of meeting future societal and industrial needs.

7 Conclusion and Future Directions

This systematic review of 82 studies provides a comprehensive understanding of the convergence of Artificial Intelligence (AI), Blockchain, and the Internet of Things (IoT) in the development of Industry 5.0 and smart city infrastructures. The analysis indicates that integrating AI for intelligent analytics, Blockchain for secure and trustworthy operations, and IoT for real-time data acquisition can substantially enhance operational efficiency, automation, resilience, and adaptability in industrial and urban systems. Practical frameworks, including Edge AI with Blockchain, Cloud AI with Hybrid Blockchain, and integrated urban models, offer tailored benefits for specific contexts, while innovations such as multi-layer smart contracts, hybrid networks, and edge–cloud computing strategies provide significant scientific and practical value.

Despite these advancements, several challenges and limitations remain. High energy consumption in computations, interoperability issues, lack of standardized protocols, and the complexity of integrating multidisciplinary technologies hinder large-scale practical deployment. Moreover, most current studies rely on simulations or limited datasets, restricting the assessment of real-world performance and system scalability. The high volume of data and the large number of sensors can also affect system efficiency, emphasizing the need for optimized and flexible solutions.

Based on these insights, future research should focus on optimizing AI algorithms and blockchain consensus mechanisms to improve energy efficiency and system responsiveness, developing standardized and modular frameworks to facilitate seamless technology integration, and implementing real-world pilot projects in industrial and urban environments for performance validation and empirical data collection. Additionally, hybrid edge–cloud computing architectures should be explored to enhance scalability, latency management, and data security, while socio-economic and human-centric considerations should be incorporated to ensure that Industry 5.0 and smart city infrastructures are sustainable, inclusive, and responsive to societal needs.

In conclusion, the convergence of AI, Blockchain, and IoT presents a transformative pathway for the next generation of industrial and urban systems. Realizing this potential requires coordinated efforts in technical optimization, standardization, multidisciplinary collaboration, and empirical validation, ultimately enabling the development of intelligent, secure, resilient, and human-centered infrastructures that define the vision of Industry 5.0 and smart cities.

Disclosure of Potential Conflicts of Interest

The Authors declare that there is no conflict of interest

Reference

[1] L. Yanytska, "The rise of human-centric manufacturing in the industry 5.0 era," Int. J. Adv. Manuf. Technol., vol. 139, no. 9, pp. 5067–5077, 2025, https://doi.org/10.1007/s00170-025-16192-5

[2] K. H. Law and J. P. Lynch, "Smart city: Technologies and challenges," IT Professional, vol. 21, no. 6, pp. 46–51, 2019, https://doi.org/10.1109/MITP.2019.2935405

[3] C. C. Liu and A. Bose, "A brief history of application of artificial intelligence to power systems," J. Mod. Power Syst. Clean Energy, vol. 14, no. 1, pp. 1–6, 2026, https://doi.org/10.35833/MPCE.2025.001004
[4] J. Ali, T. Ali, S. Musa, and A. Zahrani, "Towards secure IoT communication with smart contracts in a blockchain infrastructure," Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 10, pp. 584–591, 2018, https://doi.org/10.14569/IJACSA.2018.091070
[5] L. Mora, P. Gerli, M. Batty, E. Binet Royall, N. Carfi, K.-F. Coenegrachts, et al., "Confronting the smart city governance challenge," Nat. Cities, vol. 2, no. 2, pp. 110–113, 2025, https://doi.org/10.1038/s44284-024-00168-9
[6] M. Sverko, T. G. Grbac, and M. Mikuc, "SCADA systems with focus on continuous manufacturing and steel industry: A survey on architectures, standards, challenges and industry 5.0," IEEE Access, vol. 10, pp. 109395–109430, 2022, https://doi.org/10.1109/ACCESS.2022.3211288
[7] V. Singh, "AI-Driven Data Analytics for IoT-Based Urban Mobility Solutions," Comput. Eng. Technol. Innov., vol. 1, no. 2, pp. 114–121, 2024, https://doi.org/10.48314/ceti.v1i2.32
[8] B. Bhawana, S. Kumar, R. S. Rathore, M. Mahmud, O. Kaiwartya, and J. Lloret, "BEST—Blockchain-Enabled Secure and Trusted Public Emergency Services for Smart Cities Environment," Sensors, vol. 22, no. 15, p. 5733, 2022, https://doi.org/10.3390/s22155733
[9] K. M. K. Raghunath, M. S. Koti, R. Sivakami, V. Vinoth Kumar, G. NagaJyothi, and V. Muthukumaran, "Utilization of IoT-assisted computational strategies in wireless sensor networks for smart infrastructure management," Int. J. Syst. Assur. Eng. Manag., vol. 15, no. 1, pp. 28–34, 2024, https://doi.org/10.1007/s13198-021-01585-y
[10] N. Taleb, N. A. Al-Dmour, G. F. Issa, T. M. Abdellatif, H. M. Alzoubi, M. Alshurideh, and M. Salahat, "Analysis of Issues Affecting IoT, AI, and Blockchain Convergence," in The Effect of Information Technology on Business and Marketing Intelligence Systems, Studies in Computational Intelligence, vol. 1056, M. Alshurideh et al., Eds. Cham, Switzerland: Springer Int. Publ., 2023, pp. 2055–2066, https://doi.org/10.1007/978-3-031-12382-5_112
[11] A. I. Almulhim, "A conceptual framework for integrating IoT and blockchain for smart and sustainable urban development," Smart Cities, vol. 8, no. 6, p. 209, 2025, https://doi.org/10.3390/smartcities8060209
[12] P. Sandner, J. Gross, and R. Richter, "Convergence of blockchain, IoT, and AI," Front. Blockchain, vol. 3, p. 522600, 2020, https://doi.org/10.3389/fbloc.2020.522600
[13] T. Ramírez-Gordillo, H. Mora, A. Maciá-Lillo, S. Amador, and D. Gil, "Human-centric solutions and AI in the smart city context: the industry 5.0 perspective," in Proc. Int. Res. & Innov. Forum, Springer, Cham, 2023, pp. 193–203, https://doi.org/10.1007/978-3-031-44721-1_16
[14] P. Trakadas, P. Simoens, P. Gkonis, L. Sarakis, A. Angelopoulos, A. P. Ramallo-González, A. F. Skarmeta, C. Trochoutsos, D. Calvo, T. Pariente, K. Chintamani, I. Fernandez, A. Arnaiz Irigaray, J. X. Parreira, P. Petrali, N. Leligou, and P. Karkazis, "An artificial intelligence-based collaboration approach in industrial IoT manufacturing: Key concepts, architectural extensions and potential applications," Sensors, vol. 20, no. 19, p. 5480, 2020, https://doi.org/10.3390/s20195480
[15] R. Islam, R. Bose, S. Roy, A. A. Khan, S. Sutradhar, S. Das, F. Ali, and A. A. AlZubi, "Decentralized trust framework for smart cities: a blockchain-enabled cybersecurity and data integrity model," Sci. Rep., vol. 15, no. 1, p. 23454, 2025, https://doi.org/10.1038/s41598-025-06405-y
[16] S. Mishra and V. K. Chaurasiya, "Hybrid deep learning algorithm for smart cities security enhancement through blockchain and internet of things," Multimedia Tools Appl., vol. 83, no. 8, pp. 22609–22637, 2024, https://doi.org/10.1007/s11042-023-16406-6
[17] M. P. Loria, M. Toja, V. Carchiolo, and M. Malgeri, "An efficient real-time architecture for collecting IoT data," in Proc. 2017 Federated Conf. Comput. Sci. Inf. Syst. (FedCSIS), Prague, Czech Republic, 2017, pp. 1157–1166, https://doi.org/10.15439/2017F381
[18] Q. N. Minh, V. H. Nguyen, V. K. Quy, L. A. Ngoc, A. Chehri, and G. Jeon, "Edge computing for IoT-enabled smart grid: The future of energy," Energies, vol. 15, no. 17, p. 6140, 2022, https://doi.org/10.3390/en15176140
[19] A. Sharma, E. Podoplelova, G. Shapovalov, A. Tselykh, and A. Tselykh, "Sustainable smart cities: convergence of artificial intelligence and blockchain," Sustainability, vol. 13, no. 23, p. 13076, 2021, https://doi.org/10.3390/su132313076
[20] I. Ahmed, Y. Zhang, G. Jeon, W. Lin, M. R. Khosravi, and L. Qi, "A blockchain- and artificial intelligence-enabled smart IoT framework for sustainable city," Int. J. Intell. Syst., vol. 37, no. 9, pp. 6493–6507, 2022, https://doi.org/10.1002/int.22992
[21] A. Visvizi, R. Malik, G. M. Guazzo, and V. Çekani, "The Industry 5.0 (I50) paradigm, blockchain-based applications and the smart city," Eur. J. Innov. Manag., vol. 28, no. 1, pp. 5–26, 2025, https://doi.org/10.1108/EJIM-09-2023-0826
[22] I. González, A. J. Calderón, and J. M. Portalo, "Innovative multi-layered architecture for heterogeneous automation and monitoring systems: Application case of a photovoltaic smart microgrid," Sustainability, vol. 13, no. 4, p. 2234, 2021, https://doi.org/10.3390/su13042234
[23] A. Shankar and C. Maple, "Securing the Internet of Things-enabled smart city infrastructure using a hybrid framework," Comput. Commun., vol. 205, pp. 127–135, 2023, https://doi.org/10.1016/j.comcom.2023.04.008
[24] M. Sodhro, S. Pirbhulal, M. Muzammal, and Z. Luo, "Towards blockchain-enabled security technique for industrial Internet of Things based decentralized applications," J. Grid Comput., vol. 18, no. 4, pp. 615–628, 2020, https://doi.org/10.1007/s10723-020-09527-x
[25] A. Ed-daoudy and K. Maalmi, "A new Internet of Things architecture for real-time prediction of various diseases using machine learning on big data environment," J. Big Data, vol. 6, p. 104, 2019, https://doi.org/10.1186/s40537-019-0271-7
[26] O. A. Mahmood, A. R. Abdellah, A. Muthanna, and A. Koucheryavy, "Distributed edge computing for resource allocation in smart cities based on the IoT," Information, vol. 13, no. 7, p. 328, 2022, https://doi.org/10.3390/info13070328
[27] M. Alaeddini, M. Hajizadeh, and P. Reaidy, "A bibliometric analysis of research on the convergence of artificial intelligence and blockchain in smart cities," Smart Cities, vol. 6, no. 2, pp. 764–795, 2023, https://doi.org/10.3390/smartcities6020037
[28] B. Chander, S. Pal, D. De, and R. Buyya, "Artificial intelligence-based internet of things for Industry 5.0," in Artificial Intelligence-Based Internet of Things Systems, S. Pal, D. De, and R. Buyya, Eds., Springer, Cham, 2022, pp. 3–45, https://doi.org/10.1007/978-3-030-87059-1_1

[29] C. I. Bădoi, B. Kartal Çetin, K. Çetin, Ç. Karataş, M. E. Özbek, and S. Şahin, “A hierarchical framework leveraging IIoT networks, IoT Hub, and device twins for intelligent industrial automation,” Appl. Sci., vol. 16, no. 2, p. 645, 2026, https://doi.org/10.3390/app16020645

[30] S. Shahab, V. Simic, A. K. Dutta, D. Pamucar, and M. Anjum, “Evaluating blockchain-based waste management investments in smart cities using a multi-criteria decision support framework,” Sci. Rep., vol. 16, p. 3179, 2026, https://doi.org/10.1038/s41598-025-33085-5

[31] A. Sobecki, S. Barański, and J. Szymański, “Privacy-preserving, scalable blockchain-based solution for monitoring industrial infrastructure in the near real-time,” Appl. Sci., vol. 12, no. 14, p. 7143, 2022, https://doi.org/10.3390/app12147143

[32] S. Verma, Y. Kawamoto, Z. M. Fadlullah, H. Nishiyama, and N. Kato, “A survey on network methodologies for real-time analytics of massive IoT data and open research issues,” IEEE Commun. Surveys Tuts., vol. 19, no. 3, pp. 1457–1477, 2017, https://doi.org/10.1109/COMST.2017.2694778

[33] P. W. C. Prasad, A. Dissanayake, D. M. Nguyen, and E. Elgamal, “Sustainable and smart cities development approach with fog computing and mobile,” in Innov. Technol. Intell. Syst. Ind. Appl.: CITISIA 2024 – Vol. 1, Springer, 2026, p. 253.

[34] I. Lukić, M. Köhler, Z. Krpić, and M. Švarcmajer, “Advancing smart city sustainability through artificial intelligence, digital twin and blockchain solutions,” Technologies, vol. 13, no. 7, p. 300, 2025, https://doi.org/10.3390/technologies13070300

[35] E. Dritsas and M. Trigka, “Big data and Internet of Things applications in smart cities: recent advances, challenges, and critical issues,” Internet of Things, vol. 34, 101770, 2025, https://doi.org/10.1016/j.iot.2025.101770

[36] Y. Ghaderi and M. R. Ghaderi, “Navigating the future of smart cities: addressing IoT challenges through blockchain solutions,” Inf. Syst. Smart City, vol. 5, no. 1, p. 2334, 2025, https://doi.org/10.52963/issc.v5i1.2334

[37] A. Albugmi, “Hybrid smart IoT detection and prevention framework for smart cities using blockchain technology,” Int. J. Adv. Appl. Sci., vol. 12, no. 4, pp. 107–115, 2025, https://doi.org/10.21833/ijaas.2025.04.013

[38] B. F. Mon, M. Hayajneh, N. A. Ali, F. Ullah, H. Ullah, and S. Alkobaisi, “Digital Twins in the IIoT: Current Practices and Future Directions Toward Industry 5.0,” Comput. Mater. Contin., vol. 83, no. 3, pp. 3675–3712, 2025, https://doi.org/10.32604/cmc.2025.061411

[39] S. Salih, A. Abdelmaboud, O. Husain, A. Motwakel, H. Elshafie, M. Sharif, and M. Hamdan, “IoT in urban development: insight into smart city applications, case studies, challenges, and future prospects,” PeerJ Comput. Sci., vol. 11, p. e2816, 2025, https://doi.org/10.7717/peerj-cs.2816

[40] K. A. Robles, S. J. Delgado, and N. J. Panganiban, “Modelling Smart Cities: Integration of IoT, Big Data, and Analytics,” Int. J. Technol. Model., vol. 4, no. 3, pp. 112–127, 2025, https://doi.org/10.63876/ijtm.v4i3.160

[41] J. Brodny and M. Tutak, “Towards a Sixfold Helix Model for Green Smart Cities? A Conceptual Exploration of Stakeholder Collaboration, Interaction Mechanisms, and Role Allocation,” J. Open Innov. Technol. Mark. Complex., vol. 11, no. 4, p. 100681, 2025, https://doi.org/10.1016/j.joitmc.2025.100681

[42] Y. Ghaderi and M. R. Ghaderi, “Society 5.0 in the cloud: Harnessing the power of modern information technologies,” Metaverse Emerging Tech., 2025, https://doi.org/10.54517/m3232

[43] O. L. Rua, M. Arias-Oliva, Z. Shu, and M. Souto-Romero, “Smart cities and open innovation: what is known, how it is known and future agenda,” Discover Sustain., 2026, https://doi.org/10.1007/s43621-025-02470-5

[44] M. A. Khan, H. Menouar, and M. Abdallah, “Revisiting the intrusion detection in in-vehicle networks,” IEEE Trans. Intell. Transp. Syst., vol. 27, no. 1, pp. 333–344, 2025, https://doi.org/10.1109/TITS.2025.3628885

[45] A. Tsouplaki, C. Fung, and C. Kalloniatis, “Enhancing IoT privacy with artificial intelligence: recent advances and future directions,” Internet of Things, vol. 34, 101752, 2025, https://doi.org/10.1016/j.iot.2025.101752

[46] S. Lubis, A. Nurmandi, J. Ahmad, E. P. Purnomo, T. Purwaningsih, and H. D. Jovita-Olvez, “Synergizing AI and blockchain: a bibliometric analysis of their potential for transforming e-governance in smart cities,” Front. Sustain. Cities, vol. 7, p. 1553816, 2025, https://doi.org/10.3389/frsc.2025.1553816

[47] M. Usama, A. Aziz, N. Alasbali, N. Alturki, M. Hanif, and M. U. Rehman, “Blockchain-enabled identity management for IoT: a multi-layered defense against adversarial AI,” Sci. Rep., vol. 16, no. 1, p. 4371, 2026, https://doi.org/10.1038/s41598-026-18765-z

[48] H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, "A Review of Blockchain in Internet of Things and AI," Big Data and Cognitive Computing, vol. 4, no. 4, p. 28, 2020, https://doi.org/10.3390/bdcc4040028

[49] A. CR, A. K. Pani, and P. Kumar, "Blockchain-enabled Smart Contracts and the Internet of Things: Advancing the research agenda through a narrative review," Multimedia Tools and Applications, vol. 84, no. 8, pp. 5097-5147, 2025, https://doi.org/10.1007/s11042-024-18931-4

[50] A. Atzori, “Blockchain-based architectures for the Internet of Things: A survey,” Computer Communications, vol. 136, pp. 10–28, 2019.https://doi.org/10.1016/j.comcom.2019.01.005

[51] H.-N. Dai, Z. Zheng, and Y. Zhang,“Blockchain for Internet of Things: A survey,”IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8076–8094, 2019.https://doi.org/10.1109/JIOT.2019.2920987

[52] M. A. Khan and K. Salah,“IoT security: Review, blockchain solutions, and open challenges,”Future Generation Computer Systems, vol. 82, pp. 395–411,2018.https://doi.org/10.1016/j.future.2017.11.022

[53] M. Conoscenti, A. Vetro, and J. C. De Martin,“Blockchain for the Internet of Things: A systematic literature review,”IEEE/ACS ICPS, 2016.https://doi.org/10.1109/AICCSA.2016.7945805

[54] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke,“Blockchain technologies for the Internet of Things: Research issues and challenges,”IEEE Communications Surveys & Tutorials, 2018. https://doi.org/10.1109/COMST.2018.2866421

[55] J. Lee, B. Bagheri, and H.-A. Kao,“A cyber–physical systems architecture for Industry 4.0-based manufacturing systems,”Manufacturing Letters,3,18-23, 2015.https://doi.org/10.1016/j.mfglet.2014.12.001

[56] T. Zonta, C. A. Da Costa, R. da Rosa Righi, M. J. De Lima, E. S. Da Trindade, and G. P. Li, “Predictive maintenance in the industry 4.0: A systematic literature review, “Computers & Industrial Engineering,150,106889,2020.https://doi.org/10.1016/j.cie.2020.106889.

[57] L. Da Xu, E. L. Xu, and L. Li, “Industry 4.0: State of the art and future trends, “International Journal of Production Research,56(8),2941-2962, 2018.https://doi.org/10.1080/00207543.2018.1444806
[58] J. Leng, P. Jiang, K. Xu, Q. Liu, J. Zhou, and Y. Zhang, “Digital twin-driven manufacturing cyber–physical system, “Journal of Manufacturing Systems, 2020.https://doi.org/10.1016/j.jmsy.2019.12.003
[59] S.Nahavandi,“Industry 5.0 A human centric solution, ”Sustainability, 11(16), 4371, 2019 .https://doi.org/10.3390/su11164371
[60] L. Wang, M. Törngren, and M. Onori, “Current status and advancement of cyber-physical systems in manufacturing,” Journal of ManufacturingSystems,37,517-527,2015. https://doi.org/10.1016/j.jmsy.2015.04.008
[61] M. Javaid, A. Haleem, R. P. Singh, R. Suman, and S. Khan, “Industry 5.0: Potential applications in COVID-19 pandemic,” Journal of Industrial Integration and Management, 2020.https://doi.org/10.1142/S2424862220500220
[62] J.Xie,H. Tang, T.Huang, F.R.Yu, R.Xie, J.Liu, and Y.Liu, “A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges, ”IEEE Commun.Surv. Tutorials, vol.21, no.3, pp.2794-2830,2019. https://doi.org/10.1109/COMST.2019.2899617
[63] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and solutions,” arXiv:1608.05187, 2016.https://arxiv.org/abs/1608.05187
[64] Y. Lu, “Artificial intelligence: A survey on evolution, models, applications and future trends,” J. Manag.Analytics, vol.6, no.1, pp.1-29, 2019.https://doi.org/10.1080/23270012.2019.1570356
[65] L. U. Khan, I. Yaqoob, N. H. Tran, S. M. A. Kazmi, T. N. Dang, and C. S. Hong, “Edge-Computing-Enabled Smart Cities: A Comprehensive Survey,” IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10200–10232, Oct. 2020, https://doi.org/10.1109/JIOT.2020.2987070
[66] 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, 2020, Art. no. 102419, https://doi.org/10.1016/j.jisa.2019.102419
[67] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, “Blockchain for AI: Review and Open Research Challenges,” IEEE Access, vol. 7, pp. 10127–10149, 2019, https://doi.org/10.1109/ACCESS.2018.2890507
[68] H. Habibzadeh, K. Dinesh, O. R. Shishvan, A. Boggio-Dandry, G. Sharma, and T. Soyata, “A Survey of Healthcare Internet-of-Things (HIoT): A Clinical Perspective,” IEEE Internet of Things Journal, vol. 7, no. 1, pp. 53–71, Jan. 2020, https://doi.org/10.1109/JIOT.2019.2946359
[69] M. Veres and M. Moussa, “Deep Learning for Intelligent Transportation Systems: A Survey of Emerging Trends,” IEEE Trans. Intell. Transp. Syst., vol. 21, no. 8, pp. 3152–3168, 2020, https://doi.org/10.1109/TITS.2019.2929020
[70] X. Fang, S. Misra, G. Xue, and D. Yang, “Smart Grid — The New and Improved Power Grid: A Survey,” IEEE Commun. Surv. Tutorials, vol. 14, no. 4, pp. 944–980, 2012, https://doi.org/10.1109/SURV.2011.101911.00087
[71] Q. Yang, Y. Liu, T. Chen, and Y. Tong, “Federated Machine Learning: Concept and Applications,” ACM Trans. Intell. Syst. Technol., vol. 10, no. 2, pp. 1–19, Jan. 2019, https://doi.org/10.1145/3298981
[72] Kairouz, P., & McMahan, H. B., “Advances and open problems in federated learning”, Foundations and trends in machine learning, 2021.https://doi.org/10.1561/2200000083
[73] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, “Blockchain technology and its relationships to sustainable supply chain, “International Journal of Production Research, 2019.https://doi.org/10.1080/00207543.2018.1533261
[74] F. Tian,“An agri-food supply chain traceability system for China based on RFID & blockchain,” IEEE ICSSSM, 2016.https://doi.org/10.1109/ICSSSM.2016.7538424
[75] J. Guerrero, A. C. Chapman and G. Verbič, “Decentralized P2P energy trading under network constraints in a low-voltage network,” IEEE Trans. Smart Grid, vol. 10, no. 5, pp. 5163-5173, 2018, https://doi.org/10.1109/TSG.2018.2878445
[76] Seetah Almarri and Ahmd Aljghaiman, “Blochchin Technology for IoT Security and Trust: A Comprehensve SLR,” Sustainability, vol.16, no.23, Art.10177, Nov.2024, https://doi.org/10.3390/su162310177
[77] A. Kamilaris, A. Kartakoullis and F. X. Prenafeta-Boldú, “A review on the practice of big data analysis in agriculture,” Computers and Electronics in Agriculture, vol. 143, pp. 23-37, Dec. 2017, https://doi.org/10.1016/j.compag.2017.09.037
[78] W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu, “Edge Computing: Vision and Challenges,” IEEE Internet of Things Journal, vol. 3, no. 5,pp. 637-646, Oct. 2016, https://doi.org/10.1109/JIOT.2016.2579198
[79] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, “Internet of Things for Smart Cities,” IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22-32, Feb. 2014, https://doi.org/10.1109/JIOT.2014.2306328
[80] V. V Prabhakar, C. S. Belarmin Xavier, and K. M. Abubeker, “A Review on Challenges and Solutions in the Implementation of Ai, IoT and Blockchain in Construction Industry,” Materials Today: Proceedings, 2023, https://doi.org/10.1016/j.matpr.2023.03.535
[81] P. Pandurangan *et al.*, “Integrating cutting-edge technologies: AI, IoT, blockchain and nanotechnology for enhanced diagnosis and treatment of colorectal cancer - A review,” *Journal of Drug Delivery Science and Technology*, vol. 91, no. August 2023, p. 105197, 2024, https://doi.org/10.1016/j.jddst.2023.105197
[82] Z. Zhang, X. Song, L. Liu, J. Yin, Y. Wang, and D. Lan, "Recent advances in Blockchain and artificial intelligence integration: feasibility analysis, research issues, applications, challenges, and future work," Security and Communication Networks, vol. 2021, pp. 1-15, 2021, https://doi.org/10.1155/2021/9991535
[83] A. Nag et al., "Exploring the applications and security threats of Internet of Thing in the cloud computing paradigm: A comprehensive study on the cloud of things," Transactions on Emerging Telecommunications Technologies, vol. 35, no. 4, p. e4897, 2024, https://doi.org/10.1002/ett.4897
[84] E. Badidi, "Edge AI and Blockchain for smart sustainable cities: promise and potential," Sustainability, vol. 14, no. 13, p. 7609, 2022, https://doi.org/10.3390/su14137609
[85] P. Bothra, R. Karmakar, S. Bhattacharya, and S. De, “How can applications of blockchain and artificial intelligence improve performance of Internet of Things? – A survey,” Computer Networks, vol. 224, no. May 2021, p. 109634, 2023, https://doi.org/10.1016/j. comnet.2023.109634
[86] Z. K. Idrissi, M. Lachgar, and H. Hrimech, "Blockchain, IoT and AI in logistics and transportation: A systematic review," Transport Economics and Management, vol. 2, pp. 275-285, 2024, https://doi.org/10.1016/j.team.2024.09.002

[87] Y.Saidu, S.M.Shuhidan, D.A.Aliyu, I. Abdul Aziz, and S.Adamu,:| "Convergence of Blockchain, IoT, and AI for Enhanced Traceability System: A Comprehensive Review," IEEE Access, Vol. 13, pp.16838-16865,2025, https://doi.org/10.1109/ACCESS.2025.3528035

[88] L. Wu, W. Lu, R. Zhao, J. Xu, X. Li, and F. Xue, "Using blockchain to improve information sharing accuracy in the onsite assembly of modular construction," J. Manage. Eng., vol. 38, no. 3, Artno.04022014, May2022, https://doi.org/10.1061/(ASCE)ME.1943-5479.0001031

[89] L. Wu, W. Lu, F. Xue, X. Li, R. Zhao, and M. Tang, "Linking permissioned blockchain to Internet of Things (IoT)-BIM platform for off-site production management in modular construction," Comput. Ind., vol.135, Artno.103573, Jan.2022, https://doi.org/10.1016/j.compind.2021.103573

[90] Y. Xu, X. Tao, M. Das, H. H. Kwok, H. Liu, G. Wang, and J. C. Cheng, "Suitability analysis of consensus protocols for blockchain-based applications in the construction industry," Autom. Constr., vol.145, Artno.104638, Jan.2023,https://doi.org/10.1016/j.autcon.2022.104638

[91] R. Yang, R. Wakefield, S. Lyu, S. Jayasuriya, F. Han, X. Yi, and S. Chen, "Public and private blockchain in construction business process and information integration," Autom. Constr., vol. 118, Art no.103276, Oct. 2020, https://doi.org/10.1016/j.autcon.2020.103276

[92] Changer, S.C.G.: The Industrial Revolution from Industry 1.0 to 5.0, 2018.