Review

Future of AI-Driven IoT: Identifying Emerging Trends in Intelligent Data Analysis and Privacy Protection

Agostino Marengo *

Posted Date: 26 January 2024

doi: 10.20944/preprints202312.2184.v3

Keywords: Artificial Intelligence; Internet of Things; Integration; intelligent data analysis; privacy; emerging trends

Review

Future of AI-Driven IoT: Identifying Emerging Trends in Intelligent Data Analysis and Privacy Protection

Agostino Marengo

Department of Agricultural Sciences, Food, Natural Resources, and Engineering, University of Foggia, Foggia, Italy; agostino.marengo@unifg.it

Abstract: The integration of Artificial Intelligence (AI) with the Internet of Things (IoT) has propelled technological innovation across various industries. This systematic literature review explores the current state and future trajectories of AI in IoT, with a particular focus on emerging trends in intelligent data analysis and privacy protection. The proliferation of IoT devices, marked by voluminous data generation, has reshaped data processing methods, providing actionable insights for informed decision-making. While previous reviews have offered valuable insights, they often fall short of comprehensively addressing the multifaceted dimensions within the AI-driven IoT landscape. This review aims to bridge this gap by systematically examining existing literature and acknowledging the limitations of past studies. To achieve this aim, the study uses a meticulous approach guided by established methodologies. The chosen methodology ensures the rigor and validity of the review, aligning with PRISMA guidelines for systematic reviews. This systematic literature review serves as a comprehensive guide for researchers, practitioners, and policymakers, offering insights into the current landscape and paving the way for future research directions. The identified trends and challenges provide a valuable resource for navigating the evolving domain of AI in IoT, fostering a balanced, secure, and sustainable advancement in this dynamic field.

Keywords: Artificial Intelligence; Internet of Things; Integration; intelligent data analysis; privacy; emerging trends

1. Introduction

The Internet of Things (IoT) ecosystem encompasses an expanding network of physical devices, vehicles, household appliances, and various items embedded with electronics, software, and sensors, enabling them to connect and exchange data over the Internet. The interconnected devices in the IoT network constantly generate vast amounts of diverse and complex data. To derive useful and actionable insights, Artificial Intelligence (AI) plays a transformative role in the intelligent analysis of IoT vast datasets. AI involves the creation of computer systems capable of performing tasks that traditionally necessitate human intelligence, including learning, problem-solving, and decision-making. The AI, through intelligent analysis techniques, enables IoT devices to learn and adapt to patterns, enhancing their efficiency and functionality [1]. For instance, in smart cities, AI-driven IoT systems enable the analysis of data streams from various sensors to enhance urban planning, traffic management, and resource allocation [2]. Similarly, in an IoT-healthcare ecosystem, AI uncovers patterns in patient data, leading to personalized treatment plans and predictive healthcare analytics [3].

The synergistic coupling of AI with IoT for intelligent data analysis allows organizations to harness the potential of interconnected devices and intelligent computing systems to drive improvements in their overall performance and strategic decision-making [4]. These opportunities have created lot of interest among organizations and there are high investment projections in the AI-driven IoT landscape. For instance, the global market size for the AI-driven IoT was valued at $10.3 billion in 2022, and it is projected to reach $91.7 billion by 2032, growing at a Compound Annual

 doi:10.20944/preprints202312.2184.v3

Growth Rate (CAGR) of 24.8% [5]. McKinsey Global Institute estimates that IoT could have an economic impact of $3.9 trillion to $11.1 trillion per year by 2025, with the potential for IoT to unlock value in several settings through improved system performance and reduced costs [6, 7].

However, the convergence of AI and IoT for intelligent data analysis brings forth a significant challenge: the need to balance the power of data analysis with privacy protection [8]. As AI algorithms process and interpret sensitive information from interconnected devices, the potential for privacy breaches escalates. Consider, for instance, a smart home environment where AI systems analyze user behavior for automation – there lies a delicate balance between optimizing user experience and safeguarding individual privacy. The interconnected nature of IoT devices magnifies the impact of any lapse in privacy protection, underscoring the importance of implementing robust measures to mitigate risks. Privacy protection, therefore, becomes an imperative facet of the AI-IoT landscape. It involves not only safeguarding individual data from unauthorized access but also addressing broader ethical and legal considerations surrounding data ownership and usage. Striking the right balance between data utility for AI applications and preserving individual privacy is essential to fostering trust among users and stakeholders [9]. The implementation of privacy-preserving techniques, such as encryption, anonymization, and decentralized data processing, becomes crucial to navigating the ethical and regulatory complexities.

In essence, the synergy between intelligent data analysis and privacy protection in the context of AI and IoT is fundamental for unlocking the true potential of these technologies while ensuring ethical and responsible deployment [10]. A harmonious integration of advanced data analytics, privacy preservation measures, and AI applications not only optimizes the efficiency of IoT systems but also paves the way for a secure and trustworthy digital future. As we navigate this intricate landscape, understanding the emerging trends in intelligent data analysis and privacy protection becomes pivotal for achieving a balanced and sustainable advancement in the AI-IoT domain [11]. To achieve this, the present aims to systematically review the current body of literature pertaining to the AI-driven IoT landscape. Particularly, this study aims to find answers of the following research questions:

RQ1: *What are the emerging trends in AI-driven IoT?*
RQ2: *How does intelligent data analysis transform IoT?*
RQ3: *What are the challenges in privacy protection in AI-driven IoT?*
RQ4: *How does AI contribute to securing and managing data in IoT?*
RQ5: *What are the ethical and social implications of using AI in IoT regarding data privacy?*

Though there exist many reviews on the AI-driven IoT landscape, they reveal notable limitations that necessitate careful consideration. One recurrent limitation is the tendency of studies to adopt a narrow focus, often concentrating on specific applications e.g. healthcare, smart homes etc. within the expansive AI in the IoT spectrum [9, 12]. These focused analyses, while insightful, can inadvertently neglect the broader landscape, overlooking emerging trends and advancements that have rapidly evolved due to the swift pace of technological progress [13, 14]. Consequently, these limitations emphasize the need for a comprehensive and systematic review that not only delves into the varied applications of AI in IoT but also critically explores intelligent data analysis and privacy protection within the intricate IoT ecosystem. To fulfill this need, our review critically examines the current practices and highlights the gaps in regulatory and ethical oversight. The review also explores innovative approaches to safe-guard privacy and ethical integrity in the rapidly advancing landscape of AI-integrated IoT applications, particularly in sectors where data sensitivity is paramount. This focus provides a detailed and context-specific understanding, crucial for guiding future re-search, policy formulation, and practical implementations in this dynamic field. By doing so, this review adopts a meticulous and systematic approach and aims to provide a more nuanced understanding of the AI-driven IoT landscape, offering insights beyond the confines of specific applications and acknowledging the evolving importance of intelligent data analysis and privacy protection. The meticulous approach involves a comprehensive examination of existing literature on AI in IoT, addressing the limitations of prior studies, analysis of AI applications, intelligent data analysis, and

 doi:10.20944/preprints202312.2184.v3

privacy protection, offering a nuanced perspective on the evolving landscape of the AI-driven IoT domain

This systematic review will provide valuable contributions including shedding light on trends and advancements that may have been overlooked in the existing reviews on the AI-driven IoT. Additionally, the inclusion of intelligent data analysis and privacy protection as a focal point acknowledges the ethical considerations and potential risks associated with the integration of AI and IoT.

2. Literature Review

2.1. Evolution of AI in IoT - History and Developments

The integration of AI into IoT has marked a significant evolution in technology, with profound implications across various sectors. This journey from initial experimentation to sophisticated applications offers insight into the dynamic relationship between AI and IoT.

2.1.1. Early Developments

The In the nascent stages of AI-driven IoT, the focus gravitated towards enhancing the functionalities of IoT devices through the integration of machine learning algorithms [15]. While these early developments laid the foundation for more sophisticated integrations, the emphasis shifted towards leveraging advanced sensors and robust communication networks. The evolution of IoT took a significant leap with the introduction of AI-based sensors, marking a paradigm shift in the deployment of AI for next-generation IoT applications [16]. This progression went beyond mere device functionalities, extending into more complex and transformative applications.

A notable application emerged in the agricultural sector, where the intersection of IoT and AI revolutionized traditional farming methodologies, turning agriculture into a profitable venture [17]. This early success exemplifies the transformative potential of AI in reshaping industries and processes. As these developments unfolded, exploration expanded into the integration of cloud computing, big data, AI, and IoT, ushering in new challenges and research inquiries [18]. The trajectory moved beyond isolated technological advancements, signaling a convergence that would shape the future landscape of AI-driven IoT.

Security interfaces became a focal point with novel proposals for integrated technologies, such as a framework ensuring secure e-health services, mitigating security setbacks inherent in independent systems [19]. Simultaneously, advancements in secure smart wearable computing through AI-enabled IoT and cyber-physical systems showed promising results, especially in health monitoring applications [20]. The potential impact of these early advancements resonates in a comprehensive study discussing the integration of Blockchain, AI, and IoT technologies. This integration promised benefits like heightened security, transparency, and automation, setting the stage for the multifaceted potential of these technologies in concert [21, 22]. Furthermore, the integration of big data and AI for IoT emerged as a propellant for enhancing data transmission and processing in IoT [23]. These early forays into data integration laid the groundwork for future trends in intelligent data analysis within the AI-driven IoT ecosystem.

2.1.2. Advancements in Data Analytics

The transformative landscape of data analytics, specifically the realm of AI-driven data analytics, has been a linchpin in reshaping the dynamics of collecting and interpreting IoT data. Beyond the technical aspects, these advancements have ushered in a new era of real-time analysis and predictive capabilities, fundamentally altering the landscape of insight extraction from expansive datasets. The comprehensive investigation conducted by Mukherjee, Gupta [24] serves as an illuminating example, meticulously exploring applications and algorithms within big data analytics in 5G-enabled IoT and industrial IoT systems. This study not only offers a detailed taxonomy of existing analytical systems tailored to IoT applications but also provides a roadmap for the evolving landscape of data analytics in these contexts.

 doi:10.20944/preprints202312.2184.v3

In a practical demonstration of predictive capabilities, Salah Uddin, Asaduzzaman [25] showcase the implementation of a Smart Indoor Agriculture System, emphasizing the pragmatic utilization of predictive analysis within IoT for resource management efficiency. This exemplifies how AI-driven analytics extend beyond theoretical frameworks, finding tangible application in optimizing resource utilization. Moreover, the survey by Saadia [18] delves into the intricate integration of cloud, IoT, artificial intelligence, and big data, shedding light on emerging challenges and research issues. This work underscores the complex interplay between these technologies, emphasizing the need for a holistic understanding to propel advancements in data analytics.

Security, a paramount concern in integrated IoT technologies, is addressed by Ikharo, Obiagwu [19], who propose a novel framework for ensuring robust security in the AI, IoT, and Blockchain ecosystem. This work emphasizes that advancements in data analytics must go hand-in-hand with robust security measures to instill trust in integrated IoT systems. Additionally, the study by Ramasamy, Khan [20] showcases the efficient application of AI-enabled IoT-CPS algorithms for health monitoring, providing a tangible example of the societal impact of AI in IoT. This not only validates the practicality of AI-driven data analytics but also underscores its potential to revolutionize health monitoring, contributing to broader societal well-being.

2.1.3. Cloud and Edge Computing

The evolution of cloud computing and edge computing has facilitated large-scale processing and analysis of AI-driven data in IoT environments, addressing the challenges of data volume and computational demands [18]. Furthermore, the seamless integration of AI and IoT has opened up new possibilities for various industries, such as the fish farming industry in China, where the collaborative business ecosystem driven by AI and IoT has contributed to sustainable development, value co-creation, and digital technology-enabled sustainability [26]. Similarly, research work has focused on leveraging economic data analytic AI techniques on IoT edge devices for health monitoring in the agriculture sector, showcasing the potential for cost-effective solutions utilizing AI on edge devices [27]. Moreover, the migration of intelligence from cloud to ultra-edge smart IoT sensors using deep learning, as demonstrated in an arrhythmia monitoring use-case, exemplifies the transformative potential of integrating AI with IoT at the edge for efficient and effective monitoring systems [28]. The proposed literature review explores the impact of AI and IoT integration on the collaborative business ecosystem in the fish farming industry [29], the use of AI techniques for health monitoring in agriculture [27], and the migration of intelligence from the cloud to ultra-edge IoT sensors for arrhythmia monitoring [28].

2.1.4. Healthcare Applications

The combination of IoT, AI, and big data technologies has paved the way for remote diagnosis and treatment, significantly transforming healthcare systems [30]. Darwish, Hassanien [31] presented a comprehensive review of the current literature on the integration of cloud computing and IoT for healthcare applications, emphasizing the opportunities, challenges, and open problems in this domain. Their work offers valuable insights into the potential impact of the hybrid platform of IoT and cloud computing on healthcare systems. Furthermore, Ikharo, Obiagwu [19] proposed a novel framework for securing e-health data in the AI, IoT, and blockchain ecosystem, emphasizing the robustness and security of integrated technologies for e-health services. This work sheds light on the critical aspect of security in AI-IoT integration, particularly in the context of healthcare applications. Ramasamy et al. demonstrated the efficiency of an AI-enabled IoT-CPS algorithm in detecting patient diseases and fall events, showcasing the potential advancements in health monitoring enabled by AI-integrated IoT systems [20].

2.1.5. Governance and Ethical Considerations

The integration of AI and IoT technologies has ignited a profound focus on governance and ethical considerations, particularly within network industries [32]. This convergence has not only

 doi:10.20944/preprints202312.2184.v3

facilitated the development of novel paradigms for processing vast amounts of data and optimizing communication channels, exemplified by the emergence of 5G I-IoT [33], but has also ushered in a complex interplay among AI, robotics, and IoT over the past two decades [34]. Examining this landscape in a multidimensional manner reveals not only the growing emphasis on ethical and privacy considerations but also the multifaceted challenges faced by these aspects within the intersection of big data, AI, and the critical factor of customer trust, notably in sectors like Fintech [35].

In the realm of healthcare, the ascent of AI and big data, particularly in ophthalmology, has sparked extensive discussions on holistic approaches to address the ethical and societal challenges inherent in these technologies [36]. Moreover, the application of blockchain to devise an IoT solution for privacy-preserving big data transfer in healthcare underscores the pressing need for scalable and reliable systems, emphasizing the intricate dynamics within the convergence of AI and IoT [37].

The existing literature does not merely acknowledge the importance of ethics but delves into the verification of ethical significance, unraveling the nuanced challenges encountered. The ethical implications of AI in IoT extend beyond technological advancements, touching upon issues of data privacy, security, and societal trust. The emphasis on sectors like Fintech and healthcare illuminates the pervasive concern about the ethical and moral dimensions posed by AI. This comprehensive view of the evolution of AI in IoT reflects a journey of technological synergy marked by advancements that have redefined possibilities and continue to inspire future innovations.

2.2. Limitations and Gaps in the Existing Literature

Despite significant advancements in AI and IoT, there remain notable limitations and gaps in current research, well-documented in various studies. Taimoor and Rehman [38] provided an overview of comprehensive personalized healthcare services (CPHS) in modern healthcare Internet of Things (HIoT), highlighting the need for integrating AI in real-world scenarios. Similarly, Aitlmoudden, Housni [39] proposed a microservices-based framework for scalable data analysis in agriculture with IoT integration, emphasizing the significance of using AI in underrepresented sectors like agriculture. Furthermore, the study by Nishtar and Afzal [40] focused on real-time monitoring of hybrid energy systems using AI and IoT, addressing the scalability and sustainability challenges in AI-driven IoT systems. This research aligns with the identified gaps in the literature, emphasizing the need for more comprehensive studies that integrate AI with IoT in diverse real-world scenarios and address the scalability and sustainability of AI-driven IoT systems. Moreover, Faliagka, Panagiotou [41] presented a novel marketplace perspective promoting customized low-energy computing and IoT, which contributes to the need for more interdisciplinary research in AI-IoT solutions, aligning with the call for more holistic AI-IoT solutions. Lastly, Ataei Kachouei, Kaushik [42] reviewed state-of-the-art sensing technologies developed for food quality assurance and plant growth monitoring, addressing the limited exploration of ethical and privacy challenges in various cultural contexts. This review endeavors to bridge these gaps by integrating AI with IoT in practical applications, addressing ethical considerations and future sustainability.

3. Research Methodology

This comprehensive literature review aims to methodically explore the historical and contemporary trends in the integration of AI with IoT, focusing particularly on intelligent data analysis and privacy protection. The methodology adhered to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines, providing a well-structured and rigorous framework to ensure transparency and reproducibility.

3.1. Literature Search Strategy

The literature search strategy was designed to be exhaustive and inclusive. Key databases, including Scopus, IEEE Xplore, Springer, Web of Science, Google Scholar, Emerald, ACM, and Science Direct were used to search the relevant research articles. These databases were chosen due to

 doi:10.20944/preprints202312.2184.v3

their multidisciplinary coverage, accessibility to a diverse range of academic sources, and widespread use in systematic literature reviews.

Different search queries were designed to capture a range of articles related to different aspects of AI in IoT, including trends, challenges, applications, security, and ethical considerations. Key terms such as "AI in IoT," "Intelligent Data Analysis," and "Privacy Protection in IoT." were used with Boolean operators to refine the search and capture relevant publications. Following are a few examples of search queries.

- "Artificial Intelligence" AND "Internet of Things" AND "Emerging Trends"
- "Intelligent Data Analysis" AND "IoT" AND "Applications"
- "Privacy Protection" AND "AI in IoT" AND "Security Measures"
- "AI" AND "Internet of Things" AND "Privacy Integration"
- "Recent Advances" AND "AI in IoT"
- "Challenges" AND "AI in IoT" AND "Data Processing" OR “Intelligent Data Analysis”
- "Impact" AND "AI" AND "Privacy" AND "IoT"
- "Ethical Considerations" AND "AI in IoT" AND "Research Ethics"
- "Security Measures" AND "AI in IoT" AND "Network Security"

Table 1. Number of articles retrieved from the databases.

Database	Number of articles
Scopus	30
IEEE Xplore	12
Springer	430
Web of Science	35
Google Scholar	1020
Emerald	10
ACM	20
Science Direct	17
Total	**1574**

3.2. Inclusion and Exclusion Criteria

The criteria were carefully set to ensure that the selected articles aligned with the overarching scope of the review. This helped in minimizing bias-errors.

3.2.1. Inclusion Criteria

Language: Articles published in English.

Search Field: Scrutinize title, abstract, and keywords for relevance.

Publication Type: Full-text peer-reviewed Q1 journal articles that explicitly focused on the integration of AI-driven IoT, intelligent data analysis, and privacy protection were included.

Time Range: Encompass literature from the inception of AI in IoT to January 2024.

3.2.2. Exclusion Criteria

To maintain relevance and coherence, studies not directly related to AI, IoT, intelligent data analysis, or privacy protection were excluded. Additionally, outdated, or duplicated publications were screened out during the review process.

3.3. Publication Selection

The publication selection process involved a systematic and multi-stage approach. Initially, titles and abstracts were scrutinized to identify articles that aligned with the review's objectives. Full-text assessment followed for selected articles to ensure they met the predefined criteria, ensuring a comprehensive and focused collection of literature.

 doi:10.20944/preprints202312.2184.v3

3.4. Data Extraction

Data extraction was a meticulous process involving the systematic gathering of relevant information from selected articles. A standardized form was employed to ensure consistency in the extraction process. Information such as publication details, methodologies employed, key findings, and specific insights related to AI in IoT, intelligent data analysis, and privacy protection were systematically recorded.

3.5. Article Screening

A reference management tool i.e. EndNote 20 was employed for screening and organization of the articles. Duplicate and ineligible articles were removed. Selected articles were categorized based on their relevance to streamline subsequent analysis. This meticulous organization was used to ensure a focused and structured review process.

3.6. Quality Assessment

To ensure the methodological rigor and reliability of the review, a critical assessment of the methodological quality of each selected publication was undertaken. This involved a thorough evaluation of experimental designs, statistical methods, and overall research robustness.

3.7. Iterative Process

Recognizing the dynamic nature of research, the review embraced an iterative process. Periodic revisitation of the literature search allowed for the incorporation of newly published articles or relevant updates, ensuring the review remained current and reflective of the latest advancements. For example, if a seminal study on a new privacy protection technique in AI-driven IoT was published during the review, it was promptly incorporated into the analysis, enriching the overall synthesis.

3.8. Reporting

The final synthesis adhered to the PRISMA guidelines, offering a structured and transparent presentation of past, present, and future trajectories in AI in IoT, with specific emphasis on intelligent data analysis and privacy protection. This includes a detailed breakdown of identified trends, challenges, and opportunities, providing readers with a comprehensive and insightful overview of the evolving landscape of AI in IoT. In accordance with PRISMA, Figure 1 visually represents the number of articles included in this study, contributing to the transparency and systematic nature of our review process.

 doi:10.20944/preprints202312.2184.v3

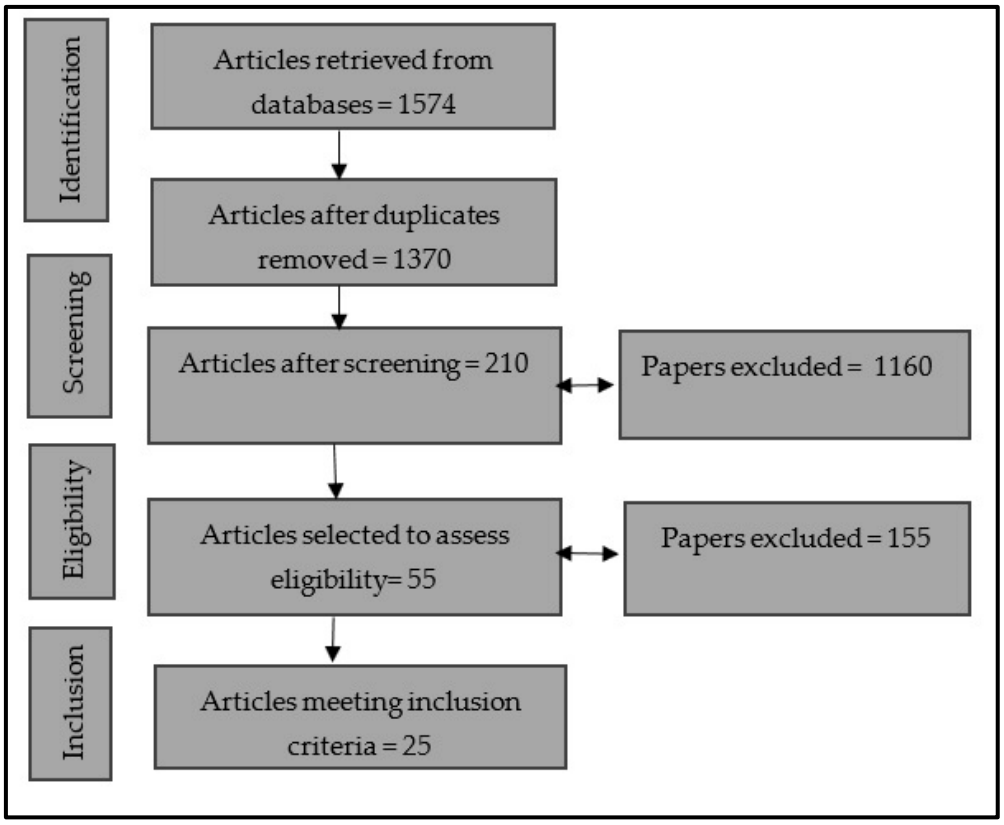

Figure 1. PRISMA flow chart.

3.9. Ethical Considerations

Throughout the entire review process, ethical considerations were paramount. Proper citation and credit were given to original authors, ensuring academic integrity, and upholding ethical standards in research conduct.

3.10. Synthesis and Analysis

The synthesis was conducted using QSR NVivo, a powerful tool for qualitative data analysis. Initially, all relevant articles identified through the systematic review were imported into NVivo, including textual data like abstracts, full articles, and supplementary materials. The node system within NVivo was then employed to create thematic categories representing key themes and concepts relevant to intelligent data analysis and privacy protection in the context of AI-driven IoT, "AI applications in IoT," "intelligent data analysis techniques," "privacy protection measures," and "emerging Trends".

The coded data was then synthesized to form a coherent narrative. This involved interpreting the data under each node, understanding how they interconnect, and constructing a narrative that encapsulates the collective insights on emerging trends related to intelligent data analysis and privacy protection in AI-driven IoT. The synthesized narrative was continuously refined and reviewed to ensure it accurately represented the data and aligned with the research aim. This iterative process not only enhanced the reliability of the synthesis but also contributed to a nuanced understanding of the identified trends in the evolving intersection of AI, IoT, intelligent data analysis, and privacy protection.

 doi:10.20944/preprints202312.2184.v3

4. Results

4.1. Key Trends

The data analysis identified several emerging trends in intelligent data analysis and privacy protection in the context of AI-driven IoT. Table 2 provides details about the key trends identified in this systematic literature review.

Table 2. Key trends identified in this systematic literature review.

Key Trend	Source	Explanation
Evolving Relationship between AI and IoT	[18],[22], [43]	The integration has led to innovations like smart exoskeleton systems and intelligent home systems. The convergence of technologies, including cloud computing, big data, and blockchain, has introduced challenges and opportunities.
Enhanced Security and Transparency	[43]	Blockchain, AI, and IoT synergies enhance security and transparency, particularly in healthcare and e-health services.
Improved Data Transmission and Processing	[23]	Integration of big data and AI enhances data transmission and processing in IoT systems.
Advancements in Smart Farming	[44]	AI, IoT, and robotics in smart farming optimize agricultural operations, leading to sustainable practices.
Integration in IP Multimedia Subsystem (IMS) Network	[11]	The convergence of AI, IoT, and ICT in the IMS network introduces innovative smart applications for advanced communication systems.
Real-time Analytics of Massive IoT Data	[45], [46]	Real-time analytics of massive IoT data, coupled with microservices-based fog computing-assisted IoT platforms, trend towards personalized and predictive data analysis.
Addressing Challenges in Knowledge Discovery	[47]	Challenges in knowledge discovery include handling missing values, data scarcity, and dimensionality reduction in IoT data processing.
Advanced Frameworks for Deep Anomaly Detection	[48]	Proposed frameworks for deep anomaly detection in industrial IoT highlight the need for sophisticated machine learning and AI techniques in IoT data processing.
Integration in Various Domains (Supply Chain, Healthcare)	[49], [50]	AI in IoT optimizes operations in supply chain management and healthcare. Intelligent processing with security intelligence enhances system efficiency.
Emphasis on Privacy and Ethical Considerations	[51], [52]	Advancements in AI with IoT necessitate a focus on privacy and ethical considerations.
Technological Trends (Edge AI, Federated Learning, etc.)	[53], [23]	Edge AI, Federated Learning, Natural Language Processes Integration, and AI-Driven Data Analytics are transforming the integration of AI with IoT.

 doi:10.20944/preprints202312.2184.v3

Applications and Case Studies	[34], [54] Integration of AI in IoT applications, such as smart home automation, healthcare, industrial processes, environmental monitoring, and transportation systems.

The evolving relationship between Artificial Intelligence (AI) and the Internet of Things (IoT) is marked by significant innovations, exemplified by the development of smart exoskeleton systems and intelligent home systems. This integration is a result of the convergence of advanced technologies, including cloud computing, big data, and blockchain. While it introduces exciting opportunities for improved efficiency and innovation, it also poses challenges related to managing the complexity of multiple technologies cohesively [18, 22, 44].

Enhanced security and transparency emerge as critical outcomes of the synergies between Blockchain, AI, and IoT, particularly evident in sectors like healthcare and e-health services. This integration enhances the overall security of data transactions and ensures transparency in the handling of sensitive information, addressing concerns related to data breaches and unauthorized access [44].

The integration of big data and AI brings about improvements in data transmission and processing within IoT systems. This trend enhances the efficiency of handling large volumes of data generated by interconnected devices, contributing to real-time data analysis and decision-making [23].

Advancements in smart farming are driven by the integration of AI, IoT, and robotics. This transformation optimizes various agricultural operations, leading to sustainable practices. Applications in smart farming include data-driven decision-making for crop management and resource utilization [44].

In the IP Multimedia Subsystem (IMS) network, the convergence of AI, IoT, and Information and Communication Technology (ICT) introduces innovative smart applications for advanced communication systems [11]. This trend facilitates the development of intelligent solutions for communication networks.

Real-time analytics of massive IoT data is a crucial trend facilitated by microservices-based fog computing-assisted IoT platforms. This approach enables personalized and predictive data analysis, providing actionable insights for informed decision-making [46, 47].

Challenges in knowledge discovery, including handling missing values, addressing data scarcity, and reducing dimensionality, are fundamental considerations in IoT data processing [47]. Overcoming these challenges is essential for extracting meaningful insights from the vast and complex datasets generated by interconnected devices.

Proposed frameworks for deep anomaly detection in industrial IoT highlight the need for sophisticated machine learning and AI techniques in data processing. These frameworks aim to improve the accuracy and efficiency of anomaly detection in industrial settings [49].

The integration of AI in various domains, such as supply chain management and healthcare, optimizes operations by leveraging intelligent processing with security intelligence. This ensures enhanced system efficiency, streamlining processes in these critical sectors [49, 50].

The emphasis on privacy and ethical considerations becomes imperative with advancements in AI within the IoT landscape. Striking a balance between utilizing data for AI applications and preserving individual privacy is crucial for fostering trust among users and stakeholders [52, 53].

Technological trends, including Edge AI, Federated Learning, Natural Language Processes Integration, and AI-Driven Data Analytics, are transformative forces in the integration of AI with IoT. These trends revolutionize real-time decision-making, enhance data security, and improve user interactions [54, 23].

Applications and case studies illustrate the diverse impact of AI in various sectors within the IoT landscape. From smart home automation to healthcare, industrial processes, environmental monitoring, and transportation systems, AI's integration paves the way for innovative solutions and enhanced efficiencies [35, 55].

 doi:10.20944/preprints202312.2184.v3

These trends collectively demonstrate the dynamic and evolving nature of the relationship between AI and IoT, presenting challenges to overcome and opportunities to explore in various domains. Each trend contributes to reshaping the landscape of intelligent data analysis and privacy protection within the AI-driven IoT ecosystem.

4.2. Future prospect and challenges

In addition to the key trends, the data analysis reveals different challenges while applying AI in IoT. Table 3 provides a comprehensive understanding of the key challenges associated with each emerging trend in AI-driven IoT, offering insights into the complexities identified in the literature review.

Table 3. Key challenges associated with AI-driven IoT.

Challenge	Source	Explanation
Real-Time Data Processing in Edge Computing	[55, 56]	Real-time data processing, fundamental to AI in IoT, faces significant hurdles in edge computing environments due to constrained processing capabilities. This limitation impedes efficient data analysis, necessitating innovative solutions for optimal performance.
Interoperability Solutions for Diverse IoT Devices	[54]	Effective communication and coordination among diverse IoT devices pose a considerable challenge, requiring advanced interoperability solutions. The complexity of data flows within IoT networks demands solutions that can seamlessly handle diverse devices and data types.
Privacy and Security Concerns in AI and IoT	[10, 56, 57]	The proliferation of IoT devices introduces heightened privacy and security concerns. With a surge in data exposure risks, safeguarding sensitive information becomes imperative.
Balancing Data Utility and User Privacy	[58, 59]	Achieving a delicate equilibrium between maximizing data utility and preserving user privacy poses a multifaceted challenge.
Infrastructure Advancements in Wireless Communication	[60, 61]	Existing common communication technologies present challenges in IoT systems, necessitating advancements in wireless communication.
Green IoT and Sustainable Outcomes	[32, 62]	The challenge lies in ensuring environmental sustainability throughout technological evolution. The emergence of 'Green IoT' signifies a proactive approach to harnessing IoT technology for environmentally sustainable outcomes.

Real-time data processing, a cornerstone of AI in IoT, is particularly challenging within edge computing environments due to limited processing capabilities, which could stymie efficient data analysis. To tackle this, Wang, Zhou [56] proposed an AI-based cloud-edge-device collaboration framework optimized through task offloading algorithms. Moreover, managing communication between diverse IoT devices demands advanced interoperability solutions capable of handling the complexity of data flows within these networks [54].

 doi:10.20944/preprints202312.2184.v3

From the privacy and security point of view, As AI and IoT technologies burgeon, they simultaneously raise significant privacy and security concerns. The proliferation of IoT devices, particularly in sensitive domains, heightens the risk of data exposure, necessitating robust encryption methods and secure data transmission protocols [10]. Federated learning models introduce unique challenges, such as susceptibility to data poisoning and evasion attacks, necessitating stringent security measures [57]. Compliance with stringent data protection regulations like GDPR is of paramount importance, as is transparency in data usage and user consent for data collection and processing [56].

To address these challenges, the literature suggests the need for innovative solutions that not only mitigate current concerns but are also adaptable to future technological advancements and threats. For instance, Bai Liu et al. propose a quantum privacy-preserving set intersection protocol for IoT, exemplifying the kind of forward-thinking required to secure IoT networks against evolving cyber threats [63].

Integrating the scholarly insights from the provided references synthesizes a narrative that underlines the urgent need for advanced solutions to the complex challenges AI and IoT face. It is evident that only through dedicated research and innovation in areas such as real-time data processing, interoperability, privacy, and security can the full potential of AI in IoT be realized in a manner that is both efficient and secure.

The IoT era, marked by an explosion in data generated by ubiquitous devices, has brought significant privacy concerns to the forefront. This is particularly challenging due to IoT's inherent nature of collecting sensitive, personal data in environments integral to our daily lives. Addressing these concerns requires practical and scalable solutions.

Innovative approaches such as federated learning and homomorphic encryption are leading these efforts. For example, Zhang, Xu [64] demonstrate a dropout-tolerable federated learning scheme in healthcare, balancing privacy with effectiveness. Similarly, Loukil, Ghedira-Guegan [65] combine blockchain with homomorphic encryption for secure IoT data aggregation in their PrivDA system. These approaches ensure data privacy while maintaining the functionality of IoT systems.

However, the challenge is not solely technological but also involves finding a balance between data utility and user privacy. Javed et al. and Lee et al. [58, 59] explore this trade-off, emphasizing the importance of social acceptance of IoT technologies. Their work highlights the complex relationship between sensor accuracy, individual comfort, and privacy considerations.

Moreover, in an increasingly privacy-conscious era, complying with regulations like GDPR is imperative. While no single solution can address every aspect of privacy protection, the combination of AI, blockchain, and encryption technologies offers a viable path forward. For instance, blockchain-based strategies for data evidence storage could enhance compliance assurance, addressing both technological and regulatory facets of privacy in IoT [66].

In summary, tackling privacy protection in IoT requires a multifaceted approach that includes practical, scalable AI techniques such as federated learning and blockchain technologies. While significant progress has been made, finding the optimal balance between utility and privacy is crucial. The role of AI in ensuring regulatory compliance in IoT is a promising area for further research and development.

Furthermore, starting from the infrastructure level, the advancements in wireless communication technologies, such as 5G and the upcoming 6G, have greatly enhanced the IoT systems' performance [60, 61]. Khanh, Hoai [60] describe a visionary perception of IoT as the primary force driving the digital revolution and mention the challenges of existing common communication technologies in IoT systems. Pattnaik, Samal [61] take this exploration a step further by discussing the application-based analysis of the 6G IoT's future, particularly for real-time location monitoring inside underground mines, an operational domain that is currently less explored. Simultaneously, attention to environmental sustainability has grown considerably in technological evolution. This is evidenced by the emergence of 'Green IoT,' where IoT technology is harnessed to promote environmentally sustainable outcomes. The short survey on 'Green IoT' offers insight into the technical evolution and future techniques to prolong the use of resources such as battery life [62].

 doi:10.20944/preprints202312.2184.v3

Furthermore, the momentous shift towards 'smart cities' indicates a convergence between AI, IoT, and Big Data, explicitly aligning with the Sustainable Development Goals (SDGs) agenda. Bibri, Alexandre [32] explain that advanced ICT has significantly influenced the manifestation of environmentally sustainable smart cities, thereby shaping the landscape and dynamics. Finally, it is imperative to mention that while these developments lead to solutions and applications that were hitherto unattainable, they also present new challenges and areas for further research. Exploring new operational domains and aligning technology with sustainability will continue to be the primary areas in the AI and IoT intersection. It's a journey that has evolved from initial experimentation to sophisticated applications and continues to transform with each step.

5. Discussion

The intersection between AI and IoT has garnered significant academic interest, resulting in several transformative applications across multiple industries. The integration's potential to revolutionize various sectors has been emphasized, such as the healthcare sector [20], credit risk evaluation innovation [67], and the automation strategy in smart cities [68]. This integration provides an enhanced customer experience and more informed business decisions through intelligent data analysis [20, 69]. The fusion of AI with IoT has not only garnered attention in academic circles but has also become a focal point for various industries. Specifically, in the healthcare sector, the integration has paved the way for transformative innovations, such as remote patient monitoring and personalized treatment plans. Moreover, the implementation of AI in credit risk evaluation has revolutionized the financial industry by enabling more accurate risk assessments and enhancing fraud detection mechanisms. Smart cities have also been at the forefront of utilizing AI in IoT to streamline automation strategies, leading to improved urban planning and resource optimization.

The interplay between AI and IoT not only enhances customer experiences but also empowers businesses to make more informed decisions through intelligent data analysis. By leveraging the data generated by IoT devices and applying AI algorithms, companies can derive invaluable insights, ultimately paving the way for enhanced operational efficiency and strategic decision-making.

Following is the discussion on the identified key trends pertaining to the research questions this study aims to answer.

RQ1: *What are the emerging trends in AI-driven IoT?*

The emergent integration of AI with IoT is forging innovative and smart systems that are finding applicability across various sectors, including healthcare. Increasingly, systems are being articulated that leverage AI, IoT, and Blockchain technologies to address the escalating complexity in today's data-driven healthcare sector [70-72]. For instance, the development of IoT-based systems like real-time respiratory rate monitoring through accelerometer sensors is aiding in remote patient monitoring [73]. In the application of patient-centric healthcare, IoMT is enhancing the scalability and effectiveness of healthcare delivery [70, 72]. The study by Satamraju and Balakrishnan [70], for instance, details how a sensor network built around IoT devices and integrated with Emotional Intelligence (EI) can help in building scalable and harmonious digital healthcare platforms. Moreover, in healthcare, the utilization of sensor data through AI and IoT can give rise to more innovative methods to face current challenges effectively. An instance is seen in the work undertaken by Onasanya and Elshakankiri [74], who emphasize the application of IoT in improving healthcare delivery by leveraging health data gathered through various sensor networks. Addressing data security in a health oriented IoT environment, many studies are exploring the potential of blockchain technology in ensuring data privacy and integrity [49, 75]. Sindhusaranya, Yamini [75] discuss federated learning and blockchain-enabled privacy-preserving systems for fraud prevention and security in IoMT. A similar perspective is shared by Atlas, Arjun [49], showcasing a decentralized privacy-preserving blockchain for IoT and big data in healthcare applications. However, Parker and Bach [76] caution about the synthesis of Blockchain, AI, and IoT, noting that while this provides scalable, secure high-level intellectual functioning, there are considerable ethical, legal, and social implications associated with these advancing technologies. The literature highlights the diverse ways that AI, IoT, and blockchain technologies are being applied in the healthcare domain. These emerging

 doi:10.20944/preprints202312.2184.v3

technologies are transforming healthcare by enabling high efficiency, advanced patient monitoring, and robust data security. However, Parker and Bach [76] stated that these advancements also demand careful consideration of the associated ethical, legal, and social implications to ensure responsible and sustainable use of technology.

RQ2: *How does intelligent data analysis transform IoT?*

The transformation of healthcare delivery systems through intelligent data analysis has become a focus of numerous studies in recent years. A prominent field of research has embraced the integration of AI and IoT in enhancing healthcare processes. One such study introduced a novel hybrid machine-learning approach for diagnosing melanoma using intelligent data analytics applied to healthcare data collected from IoT systems [77]. Similarly, recent research outlines an intelligent technique for managing and analyzing network resources within a 5G-IoT-based smart healthcare network [29]. A key concern in bridging AI and IoT in healthcare is securing and preserving the privacy of highly sensitive patient data. Several innovative approaches leveraging blockchain technology have been proposed to address these issues. For instance, Shahid, Ahmad [78] have demonstrated two encryption schemes, namely Goldwasser-Micali and Paillier, for preserving data privacy in AI applications implemented over blockchain. Another significant study has developed a hybrid Elman Neural-based Blowfish Blockchain Model to secure IoT healthcare multimedia data, enhancing confidentiality by obfuscating raw data from third-party entities. In a similar vein, a blockchain-based solution incorporating conscience identity, encryption, and decentralized storage has been suggested for securing COVID-19 testing and vaccination data [79]. Despite the several benefits of incorporating AI and IoT in healthcare systems, their ethical, legal, and social implications must not be overlooked. Media reports often represent AI as a pivot of social progress and economic development while seldom acknowledging these implications [80]. In the evolving landscape of healthcare, the confluence of IoT, blockchain, AI, and big data presents a promising pathway to enhance healthcare delivery systems. However, in order to facilitate the optimum utilization of these technologies and their successful integration into healthcare, a balance must be struck between efficiency and quality of care and the preservation of data privacy and security. Proper consideration must also be given to the ethical, legal, and social dimensions when implementing these advanced technologies in healthcare environments.

RQ3: *What are the challenges in privacy protection in AI-driven IoT?*

Privacy and data protection in IoT and AI are major areas of concern, particularly in the healthcare sector. The integration of AI with IoT offers significant opportunities to transform healthcare delivery systems, utilizing sensor devices for tracking various parameters to ensure transparency and increase vaccine coverage in remote regions [18, 20]. The use of big data and blockchain technology introduces solutions to address the challenges related to the confidentiality, security, and privacy of healthcare data. Various research has been carried out to apply blockchain technology specifically to protect the praivacy of healthcare data. For example, Healthchain was introduced as a scheme to ensure that both IoT data and doctors' diagnoses cannot be tampered with to avoid medical disputes, thereby enhancing the reliability of smart healthcare systems [18]. Other works discuss the pressing need for suitable regulatory frameworks and compliance issues within IoT devices relating to healthcare data privacy [20], and some even propose extending blockchain applications further to facilitate the secure storage of health records [84]. Moreover, the role of intelligent data analysis in transforming IoT-based healthcare systems is significant. Techniques like federated machine learning have been proposed for efficient processing within large-scale, intelligent IoT networks while still ensuring privacy [81]. Blockchain principles have also been applied within multifaceted security and privacy frameworks, thus reinforcing system security within the healthcare domain [83]. Meanwhile, certain works have highlighted the importance of privacy within e-healthcare frameworks, emphasizing the need for innovative solutions that preserve privacy alongside maintaining standard network parameters [68]. Similarly, attention has been given to the development of frameworks that use deep learning and blockchain that leverage intelligent data analysis and provide robust data security in 5G-enabled IoT systems [56]. Innovative solutions within the secure healthcare data dissemination domain have led to the proposal of multi-modal secure data

 doi:10.20944/preprints202312.2184.v3

dissemination frameworks [69]. These carefully leverage blockchain principles within the Internet of Medical Things (IoMT) to ensure secure patient data access and optimize privacy requirements. In summary, several solutions have been developed to enhance the privacy, security, and functionality of AI-driven IoT within healthcare. The proposals utilize strategies such as blockchain technology and intelligent data analysis to enhance security and confidentiality, maintain standard network parameters, and ensure robust data security in 5G-enabled systems. Future research could delve further into amplifying these strategies and managing the potential risks involved in their implementation.

RQ4: *How does AI contribute to securing and managing data in IoT?*

The contemporary discourse on the confluence of AI, IoT, big data, and blockchain technologies focuses on the potentiality of these technologies in revolutionizing various domains, with particular emphasis on the healthcare sector. The pertinence of these technologies, particularly about the protection and confidentiality of data therein, is markedly apparent. Omrčen, Leventić [82] provide a lucid exploration in their survey researching the latest blockchain solutions combined with AI technologies, aimed at improving and innovating new technical standards for the healthcare ecosystem. Their work primarily focuses on the concept of Electronic Health Records (EHR) sharing along with medical diagnostics, underlining the significant role of AI and blockchain technologies in optimizing these processes. The integration of blockchain and AI reported in the survey serves as a comprehensive model that emphasizes data privacy and security, resonating with our research interest in the use of AI in healthcare systems for secure and private data management in IoT environments. Further illustrating the promise of blockchain and AI in the healthcare sector, is the work by Parmar, Kaushik [83]. Their review explores various applications of blockchain technology in the healthcare sector with instances from public healthcare administration, patient-centered medical research, and pharmaceutical anti-counterfeiting initiatives. Even though the paper does not elaborate on the role of AI, it provides valuable insights into the rich potential of blockchain technology in health care, especially in addressing data security and privacy, which can be complemented and further enriched by AI interventions. The integration of IoT with blockchain explored by Dwivedi, Roy [84] sets a precedent for the profound impact that such a combination can have on diverse domains. In their extensive survey, they examine the need for smart contracts in IoT systems and highlight the state-of-the-art research in the convergence of blockchain and IoT. Their exploration provides a backdrop against which the multifaceted utility of these technologies for healthcare data can be appreciated. While the paper does not specifically focus on the healthcare sector, its premise is applicable and provides the rationale for examining the integrative power of these technologies with AI to address the confidentiality, security, and privacy of healthcare data. In the context of AI's potential in revolutionizing healthcare delivery systems using IoT sensor devices, these studies underscore the pertinence of integrating AI with IoT, blockchain, and big data to contribute to the field's ethical and responsible technology use. Thus, paving the road for future investigations on AI-enabled solutions for enhanced transparency and coverage in remote health care.

RQ5: *What are the ethical and social implications of using AI in IoT regarding data privacy?*

The topic of the ethical and social implications of AI in IoT, with a particular focus on healthcare and data privacy, attracted substantial scholarly attention over the past few years. According to the research [52], an Optimal Deep-Learning-Based secure blockchain (ODLSB) enabled intelligent IoT, and the healthcare diagnosis model can revolutionize healthcare to great extents, echoing our research description. This model includes secure transactions, hash value encryption, and medical diagnosis. The model is further highlighted to reinforce the security, privacy, and confidentiality of healthcare data, addressing the target ethical considerations of our research. While the use of AI and IoT can aid in creating social value and offer broader societal benefits [50], any technological innovation must be associated with due ethical considerations and privacy protection. Our research follows a similar path by aiming to provide comprehensive frameworks for the responsible and sustainable use of AI in IoT, ensuring both patients' data and privacy protection. The integration of AI, IoT, and blockchain has enormous potential to streamline healthcare operations, optimize

 doi:10.20944/preprints202312.2184.v3

resource allocation, and enhance patient outcomes. However, it is essential to construct them with careful consideration of the ethical implications anytime these technologies are applied in healthcare [52]. By ensuring the confidentiality and security of patient information, we can contribute to the development of innovative and smart healthcare systems that prioritize the security, privacy, and confidentiality of medical records. In conclusion, the integration of AI with IoT, augmented by blockchain technology, has extensive potential to transform healthcare systems. The privacy protection and data security concerns related to this integration are crucial to be addressed. In moving forward, our research aims to examine the ethical implications of this integration more deeply while developing comprehensive frameworks for its responsible and sustainable use in healthcare.

This burgeoning synergy between AI and IoT has undoubtedly opened new frontiers for innovation across diverse sectors, underscoring the need for a deeper understanding of its implications and applications. As we delve deeper into the complexities of this integration, it becomes increasingly imperative to address the ethical, legal, and social implications to ensure the responsible and sustainable use of AI in society.

However, with these advancements come crucial challenges related to ethical considerations, privacy protection, and data security. Various studies have highlighted the pressing need for robust privacy and data protection frameworks in AI-enhanced IoT systems. In addition, the ethical implications of employing AI in IoT, particularly concerning data privacy, have been underlined. For example, the introduction of AI into IoT-based healthcare systems has raised significant privacy concerns.

The application of cloud computing platforms in IoT has also been explored, demonstrating their crucial role in IT management and development. Furthermore, the integration of AI and IoT in other domains such as Fintech, edge computing, and strength training in hip-hop teaching has showcased the versatility of this fusion. In the realm of data management, the emergence of blockchain technology has surfaced as a promising tool to address the security and privacy concerns in IoT. With the proliferation of IoT devices, data security issues have become increasingly apparent, prompting the need for ecosystem-wide approaches to the problem. Consequently, Blockchain technology in IoT systems has been considered a key enabler in resolving these security issues. Nevertheless, as we further integrate AI with IoT, it becomes imperative to continue monitoring emerging trends and developments to ensure data security and privacy. This involves not only technological advancements but also the legal, ethical, and social considerations that accompany these evolving technologies.

6. Conclusions

The systematic literature review has delved into the intricate landscape of AI in IoT, exploring emerging trends in intelligent data analysis and privacy protection. Through a meticulous examination of existing literature, this review has addressed the limitations observed in past studies, offering a comprehensive understanding of the multifaceted dimensions within the AI-driven IoT landscape.

The integration of AI with IoT has witnessed remarkable advancements, as evidenced by applications ranging from smart home systems to healthcare and industrial processes. This evolution, marked by the proliferation of IoT devices and the voluminous data they generate, is reshaping data processing methods and enabling actionable insights for informed decision-making. However, this transformative journey is not without its challenges. Real-time data processing in edge computing environments poses constraints that demand innovative solutions to ensure optimal performance. The diversity of IoT devices introduces interoperability challenges, necessitating standardized communication protocols and middleware solutions. Privacy and security concerns loom large as IoT devices multiply, underscoring the need for robust security measures and privacy-preserving technologies.

As the review has highlighted, achieving a delicate equilibrium between maximizing data utility, and preserving user privacy is a multifaceted challenge requiring ongoing collaboration and dialogue among stakeholders. Advancements in wireless communication infrastructure and the

imperative of 'Green IoT' present further challenges that demand collective efforts for sustainable and efficient solutions.

This systematic literature review serves as a comprehensive guide, providing insights into the current state of AI in IoT while paving the way for future research directions. The identified trends, challenges, and potential solutions outlined herein offer a valuable resource for researchers, practitioners, and policymakers navigating the evolving landscape of AI-driven IoT. By addressing the complexities and nuances within this domain, the review contributes to fostering a balanced, secure, and sustainable advancement in the field of AI in IoT.

6.1. Research Limitations and Future Directions

While this review provides a comprehensive overview, it is not without limitations. The scope of the review is bounded by the available literature up to the knowledge cutoff date in January 2024. Newer developments post this date may not be captured, and ongoing research may introduce additional perspectives. Additionally, the review's depth may be influenced by the quality and availability of literature in the field.

To further advance the understanding of AI in IoT, future research could explore several avenues. Delving deeper into specific industry applications and their unique challenges could offer targeted solutions. Exploring the ethical dimensions of AI in IoT and developing frameworks for responsible AI deployment are critical areas for future research. Moreover, addressing the practical implementation challenges of privacy-preserving technologies and ensuring their effectiveness in real-world scenarios merits further investigation. Future research could also focus on the societal impacts of AI in IoT and strategies to mitigate potential risks.

Funding: This research received no external funding.

Data Availability Statement: by the author, available on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Kaur, N., S. Sahay, and S. Dixit, *Role of Artificial Intelligence (AI)-aided Internet of Things (IoT) Technologies in Business and Production*, in *Advanced IoT Technologies and Applications in the Industry 4.0 Digital Economy*. 2024, CRC Press. p. 29-41.
2. Kannammal, A. and S. Chandia, *Applications of AI and IoT for Smart Cities.* Research Trends in Artificial Intelligence: Internet of Things, 2023: p. 186.
3. Hema, D., *Smart healthcare IoT Applications Using AI*, in *Integrating AI in IoT Analytics on the Cloud for Healthcare Applications*. 2022, IGI Global. p. 238-257.
4. Balas, V.E., R. Kumar, and R. Srivastava, *Recent trends and advances in artificial intelligence and internet of things*. 2020: Springer.
5. Dhapte, A. *Generative AI Market Overview*. 2024 [cited 2024; Available from: https://www.marketresearchfuture.com/reports/generative-ai-market-11879.
6. Chui, M., M. Collins, and M. Patel, *IoT value set to accelerate through 2030: Where and how to capture it*. 2021, McKinsey.
7. Manyika, J., et al., *Unlocking the potential of the Internet of Things*. 2015, McKinsey Global Institute.
8. Shi, F., et al., *Recent progress on the convergence of the Internet of Things and artificial intelligence.* IEEE Network, 2020. **34**(5): p. 8-15.
9. Sepasgozar, S., et al., *A systematic content review of artificial intelligence and the internet of things applications in smart home.* Applied Sciences, 2020. **10**(9): p. 3074.
10. Singh, P.D. and K.D. Singh, *Security and Privacy in Fog/Cloud-based IoT Systems for AI and Robotics.* EAI Endorsed Transactions on AI and Robotics, 2023. **2**.
11. Tsai, J.-W., et al. *The Smart Applications of ICT and IoT with AI Techniques in IMS Network*. in *2023 24st Asia-Pacific Network Operations and Management Symposium (APNOMS)*. 2023. IEEE.
12. Alshehri, F. and G. Muhammad, *A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare.* IEEE Access, 2020. **9**: p. 3660-3678.
13. Borgia, E., *The Internet of Things vision: Key features, applications and open issues.* Computer Communications, 2014. **54**: p. 1-31.

14. Atzori, L., A. Iera, and G. Morabito, *The internet of things: A survey.* Computer networks, 2010. **54**(15): p. 2787-2805.
15. Jamil, F., et al., *Towards secure fitness framework based on IoT-enabled blockchain network integrated with machine learning algorithms.* Sensors, 2021. **21**(5): p. 1640.
16. Mukhopadhyay, S.C., et al., *Artificial intelligence-based sensors for next generation IoT applications: A review.* IEEE Sensors Journal, 2021. **21**(22): p. 24920-24932.
17. Agarwal, K., et al. *Intelligence and Internet of Things with 5G Technology: Application and Development*. in *2022 International Conference on Electronics and Renewable Systems (ICEARS)*. 2022. IEEE.
18. Saadia, D., *Integration of cloud computing, big data, artificial intelligence, and internet of things: Review and open research issues.* International Journal of Web-Based Learning and Teaching Technologies (IJWLTT), 2021. **16**(1): p. 10-17.
19. Ikharo, B., et al. *Security for Internet-of-Things Enabled E-Health using Blockchain and Artificial Intelligence: A Novel Integration Framework*. in *2021 1st International Conference on Multidisciplinary Engineering and Applied Science (ICMEAS)*. 2021. IEEE.
20. Ramasamy, L.K., et al., *Secure smart wearable computing through artificial intelligence-enabled internet of things and cyber-physical systems for health monitoring.* Sensors, 2022. **22**(3): p. 1076.
21. Marengo, A. and A. Pagano, *Investigating the factors influencing the adoption of blockchain technology across different countries and industries: a systematic literature review.* Electronics, 2023. **12**(14): p. 3006.
22. Aruna, S., et al. *Blockchain Integration with Artificial Intelligence and Internet of Things Technologies*. in *2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS)*. 2023. IEEE.
23. Wei, W., et al., *Guest editorial: special section on integration of big data and artificial intelligence for internet of things.* 2020.
24. Mukherjee, S., et al., *Leveraging big data analytics in 5G-enabled IoT and industrial IoT for the development of sustainable smart cities.* Transactions on Emerging Telecommunications Technologies, 2022. **33**(12): p. e4618.
25. Salah Uddin, M., et al. *Implementation of smart indoor agriculture system and predictive analysis*. in *Advances in Computing and Data Sciences: Third International Conference, ICACDS 2019, Ghaziabad, India, April 12–13, 2019, Revised Selected Papers, Part I 3*. 2019. Springer.
26. Yang, X., et al., *AI and IoT-based collaborative business ecosystem: A case in Chinese fish farming industry.* International Journal of Technology Management, 2020. **82**(2): p. 151-171.
27. Gupta, N., et al., *Economic data analytic AI technique on IoT edge devices for health monitoring of agriculture machines.* Applied Intelligence, 2020. **50**: p. 3990-4016.
28. Sakib, S., et al. *Migrating intelligence from cloud to ultra-edge smart IoT sensor based on deep learning: An arrhythmia monitoring use-case*. in *2020 International Wireless Communications and Mobile Computing (IWCMC)*. 2020. IEEE.
29. Yang, K., et al., *Federated machine learning for intelligent IoT via reconfigurable intelligent surface.* IEEE network, 2020. **34**(5): p. 16-22.
30. Najim, A.H., et al. *The impact of using IoT for elderly and disabled peoples healthcare: An overview*. in *2022 2nd International Conference on Computing and Information Technology (ICCIT)*. 2022. IEEE.
31. Darwish, A., et al., *The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems.* Journal of Ambient Intelligence and Humanized Computing, 2019. **10**: p. 4151-4166.
32. Bibri, S.E., et al., *Environmentally sustainable smart cities and their converging AI, IoT, and big data technologies and solutions: an integrated approach to an extensive literature review.* Energy Informatics, 2023. **6**(1): p. 9.
33. Aggarwal, N. and D. Singh. *Technology assisted farming: Implications of IoT and AI*. in *IOP Conference Series: Materials Science and Engineering*. 2021. IOP Publishing.
34. Börner, K., et al., *Mapping the co-evolution of artificial intelligence, robotics, and the internet of things over 20 years (1998-2017).* PloS one, 2020. **15**(12): p. e0242984.
35. Aldboush, H.H. and M. Ferdous, *Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust.* International Journal of Financial Studies, 2023. **11**(3): p. 90.
36. Liu, T. and J.-H. Wu, *The Ethical and Societal Considerations for the Rise of Artificial Intelligence and Big Data in Ophthalmology.* Frontiers in Medicine, 2022. **9**: p. 845522.
37. Elhoseny, M., et al., *IoT solution for AI-enabled PRIVACY-PREServing with big data transferring: an application for healthcare using blockchain.* Energies, 2021. **14**(17): p. 5364.
38. Taimoor, N. and S. Rehman, *Reliable and resilient AI and IoT-based personalised healthcare services: A survey.* IEEE Access, 2021. **10**: p. 535-563.
39. Aitlmoudden, O., et al., *A Microservices-based Framework for Scalable Data Analysis in Agriculture with IoT Integration.* International Journal of Interactive Mobile Technologies, 2023. **17**(19).

40. Nishtar, Z. and J. Afzal, *A Review of Real-Time Monitoring of Hybrid Energy Systems by Using Artificial Intelligence and IoT.* Pakistan Journal of Engineering and Technology, 2023. **6**(3): p. 8-15.
41. Faliagka, E., et al. *A Novel Marketplace Perspective Promoting Customized Low Energy Computing and IoT: The SMART4ALL Approach*. in *2022 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. 2022. IEEE.
42. Ataei Kachouei, M., A. Kaushik, and M.A. Ali, *Internet of Things-Enabled Food and Plant Sensors to Empower Sustainability.* Advanced Intelligent Systems, 2023: p. 2300321.
43. Yukitake, T. *Innovative solutions toward future society with AI, Robotics, and IoT*. in *2017 Symposium on VLSI Circuits*. 2017. IEEE.
44. Pal, D. and S. Joshi. *AI, IoT and Robotics in Smart Farming: Current Applications and Future Potentials*. in *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*. 2023. IEEE.
45. Verma, S., et al., *A survey on network methodologies for real-time analytics of massive IoT data and open research issues.* IEEE Communications Surveys & Tutorials, 2017. **19**(3): p. 1457-1477.
46. Taneja, M., et al., *SmartHerd management: A microservices-based fog computing–assisted IoT platform towards data-driven smart dairy farming.* Software: practice and experience, 2019. **49**(7): p. 1055-1078.
47. Al-Janabi, S. *Overcoming the main challenges of knowledge discovery through tendency to the intelligent data analysis*. in *2021 International Conference on Data Analytics for Business and Industry (ICDABI)*. 2021. IEEE.
48. Nizam, H., et al., *Real-time deep anomaly detection framework for multivariate time-series data in industrial iot.* IEEE Sensors Journal, 2022. **22**(23): p. 22836-22849.
49. Atlas, L.G., K. Arjun, and B. Babu, *A Decentralized Privacy-Preserving Blockchain for IoT and Big Data in Healthcare Applications*, in *Convergence of Blockchain, AI, and IoT*. 2021, CRC Press. p. 19-32.
50. Mochizuki, Y. *AI and IoT for social value creation*. in *2019 IEEE Asian Solid-State Circuits Conference (A-SSCC)*. 2019. IEEE.
51. Pervaiz, A., et al., *Incorporating noise robustness in speech command recognition by noise augmentation of training data.* Sensors, 2020. **20**(8): p. 2326.
52. Veeramakali, T., et al., *An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model.* The Journal of Supercomputing, 2021: p. 1-21.
53. Sepasgozar, S., et al., *Introductory Chapter: Intelligence, Sustainable and Post-COVID-19 Resilience Built Environment: An Agenda for Future*, in *Design of Cities and Buildings-Sustainability and Resilience in the Built Environment*. 2021, IntechOpen.
54. Lagkas, T., et al., *UAV IoT framework views and challenges: Towards protecting drones as "Things"*. Sensors, 2018. **18**(11): p. 4015.
55. Wang, Y., et al., *Distributed Swarm Learning for Internet of Things at the Edge: Where Artificial Intelligence Meets Biological Intelligence.* arXiv preprint arXiv:2210.16705, 2022.
56. Wang, Z., et al., *AI-based cloud-edge-device collaboration in 6G space-air-ground integrated power IoT.* IEEE Wireless Communications, 2022. **29**(1): p. 16-23.
57. Rahman, M.A., et al., *Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city.* Ieee Access, 2019. **7**: p. 18611-18621.
58. Javed, A.R., et al., *Integration of blockchain technology and federated learning in vehicular (iot) networks: A comprehensive survey.* Sensors, 2022. **22**(12): p. 4394.
59. Lee, A.J., J.T. Biehl, and C. Curry. *Sensing or watching? Balancing utility and privacy in sensing systems via collection and enforcement mechanisms*. in *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*. 2018.
60. Khanh, Q.V., et al., *Wireless communication technologies for IoT in 5G: Vision, applications, and challenges.* Wireless Communications and Mobile Computing, 2022. **2022**: p. 1-12.
61. Pattnaik, S.K., et al., *Future wireless communication technology towards 6g IoT: an application-based analysis of IoT in real-time location monitoring of employees inside underground mines by using BLE.* Sensors, 2022. **22**(9): p. 3438.
62. Popli, S., R.K. Jha, and S. Jain, *Green IoT: A short survey on technical evolution & techniques.* Wireless Personal Communications, 2022: p. 1-29.
63. Liu, B., et al., *SEPSI: A Secure and Efficient Privacy-Preserving Set Intersection with Identity Authentication in IoT.* Mathematics, 2022. **10**(12): p. 2120.
64. Zhang, L., et al., *Homomorphic encryption-based privacy-preserving federated learning in iot-enabled healthcare system.* IEEE Transactions on Network Science and Engineering, 2022.
65. Loukil, F., et al., *Privacy-preserving IoT data aggregation based on blockchain and homomorphic encryption.* Sensors, 2021. **21**(7): p. 2452.
66. Gao, Y., Z. Huang, and J. He. *Privacy-preserving and verifiable IoT data aggregation scheme based on blockchain and homomorphic encryption*. in *3rd International Conference on Artificial Intelligence, Automation, and High-Performance Computing (AIAHPC 2023)*. 2023. SPIE.

67. Bi, W. and Y. Liang, *Risk Assessment of Operator's Big Data Internet of Things Credit Financial Management Based on Machine Learning*. Mobile Information Systems, 2022. **2022**.
68. Ezzat, M.A., et al., *Horizontal review on video surveillance for smart cities: Edge devices, applications, datasets, and future trends.* Sensors, 2021. **21**(9): p. 3222.
69. Reddy, B.K., et al., *Latest trends and their adoptions in electrical power systems-an industrial perspective.* Indonesian Journal of Electrical Engineering and Computer Science, 2023. **29**(1): p. 8-14.
70. Satamraju, K.P. and M. Balakrishnan, *A secured healthcare model for sensor data sharing with integrated emotional intelligence.* IEEE Sensors Journal, 2022. **22**(16): p. 16306-16313.
71. Junaid, S.B., et al. *Recent advancements in emerging technologies for healthcare management systems: A survey*. in *Healthcare*. 2022. MDPI.
72. Gomathi, L., A.K. Mishra, and A.K. Tyagi. *Industry 5.0 for Healthcare 5.0: Opportunities, Challenges and Future Research Possibilities*. in *2023 7th International Conference on Trends in Electronics and Informatics (ICOEI)*. 2023. IEEE.
73. Andarevi, M.H. and A.A. Iskandar. *A Prototype of IoT-based Real-time Respiratory Rate Monitoring Using an Accelerometer Sensor*. in *2022 4th International Conference on Biomedical Engineering (IBIOMED)*. 2022. IEEE.
74. Onasanya, A. and M. Elshakankiri. *Secured cancer care and cloud services in IoT/WSN based medical systems*. in *Smart Grid and Internet of Things: Second EAI International Conference, SGIoT 2018, Niagara Falls, ON, Canada, July 11, 2018, Proceedings 2*. 2019. Springer.
75. Sindhusaranya, B., et al., *Federated Learning and Blockchain-Enabled Privacy-Preserving Healthcare 5.0 System: A Comprehensive Approach to Fraud Prevention and Security in IoMT.* Journal of Internet Services and Information Security, 2023.
76. Parker, B. and C. Bach, *The synthesis of blockchain, artificial intelligence and internet of things.* European Journal of Engineering and Technology Research, 2020. **5**(5): p. 588-593.
77. Mani, V., et al., *Hyperledger healthchain: patient-centric IPFS-based storage of health records.* Electronics, 2021. **10**(23): p. 3003.
78. Shahid, J., et al., *Data protection and privacy of the internet of healthcare things (IoHTs).* Applied Sciences, 2022. **12**(4): p. 1927.
79. Jiang, F., et al. *Federated Learning-Based Privacy Protection for IoT-based Smart Healthcare Systems*. in *2023 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*. 2023. IEEE.
80. Xu, J., et al., *Healthchain: A blockchain-based privacy preserving scheme for large-scale health data.* IEEE Internet of Things Journal, 2019. **6**(5): p. 8770-8781.
81. Liu, J. and W. Ren, *The Application of Edge Computing Technology in Strength Training in Hip-Hop Training and Teaching under the Background of Artificial Intelligence and Internet of Things.* Wireless Communications and Mobile Computing, 2022. **2022**.
82. Omrčen, L., et al. *Integration of Blockchain and AI in EHR sharing: A survey*. in *2021 International Symposium ELMAR*. 2021. IEEE.
83. Parmar, J., G. Kaushik, and P. Sharma, *An Application of Blockchain: A Review.* Tuijin Jishu/Journal of Propulsion Technology, 2023.
84. Dwivedi, S.K., et al., *Blockchain-based internet of things and industrial IoT: A comprehensive survey.* Security and Communication Networks, 2021. **2021**: p. 1-21.