Review

The Future of AI in IoT: Emerging Trends in Intelligent Data Analysis and Privacy Protection

Agostino Marengo *

Posted Date: 28 December 2023

doi: 10.20944/preprints202312.2184.v1

Keywords: Artificial Intelligence; Internet of Things; AI-IoT Integration; Intelligent Data Analysis; Privacy Protection in IoT; Blockchain Technology

Review

The Future of AI in IoT: 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: This paper explores the dynamic intersection of Artificial Intelligence (AI) and the Internet of Things (IoT), focusing on emerging trends in intelligent data analysis and privacy protection. Employing a systematic literature review, we analyze recent advancements and challenges in AI-IoT integration. The paper highlights key developments in sensor data anomaly detection, AI-driven big-data analytics, and IoT-based communication techniques. It delves into the complexities of privacy protection in IoT, examining innovative solutions like federated learning and blockchain technologies. The study also addresses the challenges in AI for IoT, prioritizing the most pressing issues such as data security, ethical implementation, and compliance with regulations like GDPR. The research underscores the need for adaptable solutions that balance technological advancements with privacy and security considerations, setting a path for future exploration in AI-empowered IoT applications.

Keywords: artificial intelligence; internet of things; AI-IoT integration; intelligent data analysis; privacy protection in IoT; blockchain technology

1. Introduction

The integration of Artificial Intelligence with the Internet of Things and 5G technologies represents a pivotal advancement in the technological landscape, presenting a multitude of opportunities for innovation across various sectors. The global AI in IoT market size was valued at $10.3 billion in 2022, and it is projected to reach $91.7 billion by 2032, growing at a compound annual growth rate (CAGR) of 24.8% [42].

As this integration continues to reshape industries and drive business decisions, it is crucial to address the ethical and privacy challenges that accompany this rapid evolution. The burgeoning potential of AI to revolutionize customer experiences and enable intelligent data analysis is undeniable, but it necessitates a concurrent focus on robust privacy and data protection measures. A study from 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. Furthermore, Boston Consulting Group (BCG) reported a case where the integration of AI with IoT helped a client achieve a 30% reduction in repair times, increasing the productivity of field workers and improving equipment functionality. Moreover, a report by Accenture states that AI could increase business productivity by up to 40% by 2035, and implementing AI could lead to a reduction in manufacturing costs by 20%.

The seamless integration of AI with emerging technologies, including blockchain and augmented reality, has unlocked a wave of innovation, fostering creative applications and transformative solutions. While this convergence offers immense benefits, it also introduces significant challenges and risks that must be carefully navigated. The ethical, legal, and social implications of this widespread adoption of AI require thorough consideration to ensure responsible and sustainable use in society.

Understanding the latest trends, developments, and applications of AI is critical for researchers, practitioners, and policymakers to effectively navigate this complex terrain. It is imperative to analyze emerging innovations and future directions in the use of AI in IoT, identify the most impactful AI technologies in the IoT landscape, and explore how intelligent data analysis is

 doi:10.20944/preprints202312.2184.v1

transforming IoT systems. The AI in IoT market is projected to grow from USD 8.3 Billion in 2023 to USD 60.8 Billion by 2032, exhibiting a CAGR of 28.20% during the forecast period (2023 - 2032) [43].

M.J. Baucas et al. [9] in their study "Federated Learning and Blockchain-Enabled Fog-IoT Platform for Wearables in Predictive Healthcare" cite a relevant case study addressing the integration of AI for privacy protection revolves around the use of smart meters. These devices collect detailed energy usage data that, when analyzed by AI, can reveal sensitive personal information such as household habits and income levels. The study emphasizes the privacy risks associated with advanced AI technologies' capability to interpret extensive and detailed data sets. It also questions the sufficiency of current privacy legislation to protect consumers against the invasive potential of AI-driven data analysis. To tackle these issues, the study proposes novel solutions aimed at enhancing privacy protection for consumers.

Two other case studies demonstrating the effectiveness of AI in IoT are made from Frito-Lay (PepsiCo subsidiary) [20] and Smart Traffic Management in Singapore [18]. The first one uses machine learning to automate quality checks of chips by analyzing the sound produced by lasers hitting the chips to determine texture. AI is also used to predict potato weights, which has eliminated the need for expensive weighing elements, and an ongoing project assesses the "percent peel" of potatoes after peeling, potentially saving over $1 million annually in the U.S. alone. In the second case study, the city of Singapore has implemented an AI-driven traffic management system. The system uses sensors and cameras to collect real-time traffic data, which AI algorithms then analyze to optimize traffic flow and reduce congestion. It has significantly improved commute times and reduced pollution from idling vehicles.

Furthermore, addressing the challenges and opportunities presented by privacy protection in AI-enhanced IoT, and assessing the ethical and social implications of using AI in IoT, particularly regarding data privacy, are essential to chart the path forward in this dynamic field.

2. Main Focus of the Review

The ethical and privacy challenges in AI and IoT integration are multifaceted and evolving. This review delves into the specific ethical dilemmas and privacy concerns unique to this technological convergence. We focus on the pressing need for developing sophisticated data security frameworks and ethical guidelines tailored to the nuances of AI-driven IoT systems. Our analysis includes a critical examination of current practices, highlighting the gaps in regulatory and ethical oversight. The review also explores innovative approaches to safeguard 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 research, policy formulation, and practical implementations in this dynamic field.

3. Review Methodology

In this literature review, we employed a structured approach to select and analyze pertinent sources, adhering to specific criteria for source selection. We reviewed 88 articles and we included studies published within the last six years to ensure the information's relevance and timeliness. The focus was on articles from Q1 journals, which are recognized for their high impact in the fields of AI and IoT. The citation volume of these studies was also considered as an indicator of their significance in the field. Our research utilized renowned academic databases like IEEE Xplore, Scopus, and Web of Science. Searches were conducted using keywords such as "AI in IoT," "Intelligent Data Analysis," and "Privacy in IoT." The selection process was not solely quantitative; we also evaluated the content of the articles to confirm their direct relevance to "intelligent data analysis" and "privacy protection" in AI and IoT. Each chosen article underwent a critical evaluation to understand its approach, methods, results, and conclusions. We organized and synthesized this information thematically to provide a comprehensive overview of current trends, challenges, and opportunities in AI applied to IoT. Our methodology was iterative, involving continuous updating with new studies, ensuring the review remained current, informative, and of high quality.

 doi:10.20944/preprints202312.2184.v1

Key Research Questions

In this sub-section, the different research questions will be highlighted, which will serve as the primary point of interest and focus in this research. The five research questions being highlighted in this study are given below:

1. What are the latest emerging trends in integrating Artificial Intelligence (AI) with the Internet of Things (IoT)? Examine recent innovations and future directions in the use of AI in IoT. Identify which AI technologies are having the most significant impact on IoT.

2. How is intelligent data analysis transforming IoT? Explore how advanced AI-based data analytics techniques are enhancing the functionality and efficiency of IoT systems. Discuss specific examples where AI-driven data analysis has led to significant improvements.

3. What challenges and opportunities does privacy protection present in AI-enhanced IoT? Analyze the current challenges in data and privacy protection in AI-enabled IoT. Explore emerging solutions and strategies to address these challenges.

4. How can AI contribute to more secure and private data management in IoT? Investigate AI techniques that promote data security and privacy in IoT. Assess the effectiveness of these techniques in real-world scenarios.

5. What are the ethical and social implications of using AI in IoT, particularly regarding data privacy? Discuss the ethical considerations related to the use of AI in IoT, with a focus on data privacy. Reflect on the social implications and public acceptance of these technologies.

4. Evolution of AI in IOT - History and Developments

The integration of Artificial Intelligence (AI) into the Internet of Things (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.

4.1. Early Developments

The initial focus was on enhancing IoT device functionalities through machine learning algorithms [27]. This laid the groundwork for more complex integrations, leveraging advanced sensors and reliable communication networks. The evolution of IoT towards sophisticated applications has been reinforced by the advent of AI-based sensors, which enable the deployment of AI for next-generation IoT applications [47]. Furthermore, the intersection of IoT and AI has revolutionized traditional agriculture methodologies, making farming a profitable venture [1]. Recent developments in the field have also explored the integration of cloud computing, big data, AI, and IoT, leading to new challenges and research issues [61]. Moreover, there have been novel proposals for integrated technology's security interfaces, such as a framework for secure e-health services that lessens security setbacks in independent ones [26]. Additionally, secure smart wearable computing through AI-enabled IoT and cyber-physical systems has shown promising results for health monitoring [58]. The potential impact of these advancements has been further highlighted in a comprehensive study that discusses the integration of Blockchain, AI, and IoT technologies and their benefits, including increased security, transparency, and automation [7,41]. Furthermore, the integration of big data and AI for IoT has been identified as a propellant to improve data transmission and processing in IoT [89].

4.2. Advancements in Data Analytics

Advancements in Data Analytics, particularly AI-driven data analytics, have played a pivotal role in transforming the collection and interpretation of IoT data. Real-time analysis and predictive capabilities have emerged, enabling the extraction of insightful patterns from vast datasets [46]. The study by Mukherjee et al. [46] provides an exhaustive investigation into the various applications and algorithms of big data analytics in 5G-enabled IoT and industrial IoT systems, offering a detailed taxonomy of existing analytical systems specific to IoT applications. In addition, the work presented

 doi:10.20944/preprints202312.2184.v1

by Uddin et al. [77] focuses on the implementation of a Smart Indoor Agriculture System with predictive analysis, showcasing the practical utilization of predictive capabilities in IoT for efficient resource management [77]. Furthermore, the survey by Saadia [61] sheds light on the integration of cloud, IoT, artificial intelligence, and big data, highlighting new challenges and research issues, underscoring the complex interplay between these technologies [61]. Moreover, Ikharo et al. [26] propose a novel framework for the security of e-health data in the AI, IoT, and Blockchain ecosystem, emphasizing the significance of ensuring robust security in integrated IoT technologies [26]. Additionally, the study by Ramasamy et al. demonstrates the efficient use of AI-enabled IoT-CPS algorithms for health monitoring, indicating the practical application of AI in IoT for significant societal impact [58,65].

4.3. 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 [61]. 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 [81]. 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 [24]. 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 [64]. The proposed literature review explores the impact of AI and IoT integration on the collaborative business ecosystem in the fish farming industry [81], the use of AI techniques for health monitoring in agriculture [24], and the migration of intelligence from the cloud to ultra-edge IoT sensors for arrhythmia monitoring [64].

4.4. Healthcare Applications

The combination of IoT, AI, and big data technologies has paved the way for remote diagnosis and treatment, significantly transforming healthcare systems [48]. Darwish et al. 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 [13]. Their work offers valuable insights into the potential impact of the hybrid platform of IoT and cloud computing on healthcare systems. Furthermore, Ikharo et al., as said 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 [26]. 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 [58].

4.5. Governance and Ethical Considerations

The convergence of AI and IoT technologies has brought about a growing focus on governance and ethical considerations related to big data and AI in network industries [11]. This integration has also given rise to the development of new paradigms for processing large amounts of data and optimizing communication channels, as seen in the emergence of 5G I-IoT [2]. The co-evolution of AI, robotics, and IoT over the last two decades has brought attention to the complex dynamics and interplay among these technological domains [12]. The need to address ethical and privacy considerations in the intersection of big data, AI, and customer trust has become increasingly prominent, particularly in sectors such as Fintech [4]. Additionally, the rise of AI and big data in the

 doi:10.20944/preprints202312.2184.v1

field of ophthalmology has prompted discussions around comprehensive approaches to tackle ethical and societal challenges associated with these technologies [38]. Furthermore, the application of blockchain to create an IoT solution for privacy-preserving big data transfer in the healthcare sector highlights the need for scalable and reliable systems within the context of AI and IoT convergence [15].

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.

5. Current Trends, Challenges, and Issues

The evolving relationship between AI and IoT has yielded innovative solutions, such as smart exoskeleton systems for rehabilitation and intelligent home systems, demonstrating the diverse applications arising from this integration [85]. This evolution has been facilitated by the convergence of advanced technologies, including cloud computing, big data, and blockchain, which have introduced new challenges and research opportunities [7,61]. Furthermore, the combined capabilities of blockchain, AI, and IoT have been highlighted to enhance security and transparency in various industries, including healthcare and e-health services [85]. The integration of big data and AI for IoT has also been recognized as a propellant for improving data transmission and processing, underscoring the potential for enhanced data management and analysis in IoT systems [89]. Moreover, the application of AI, IoT, and robotics in smart farming has opened new horizons for sustainable agriculture, paving the way for future advancements in the industry [53]. Notably, the convergence of AI, IoT, and ICT in the IP Multimedia Subsystem (IMS) network has introduced innovative smart applications, offering solutions for advanced communication systems [76].

5.1. Trends

The integration of artificial intelligence with the Internet of Things (IoT) has catalyzed notable advancements in intelligent data analysis. This evolution, marked by the burgeoning of IoT devices and the voluminous data they generate, is not only reshaping data processing methods but also enabling actionable insights for informed decision-making.

Key developments in this arena include real-time analytics of massive IoT data and the implementation of microservices-based fog computing-assisted IoT platforms. For instance, Verma et al. [79] and Taneja et al. [75] explore network methodologies and practical applications like "SmartHerd management" for data-driven dairy farming. These advancements underscore the trend towards personalized and predictive data analysis.

Moreover, the challenges in knowledge discovery, particularly in handling missing values, data scarcity, and dimensionality reduction, are crucial in processing IoT data volumes, as discussed by Al-Janabi [3]. Concurrently, Nizam et al. [50] propose advanced frameworks for deep anomaly detection in industrial IoT, demonstrating the need for sophisticated machine learning and AI techniques in IoT data processing.

The transformative role of AI in IoT extends to various domains, optimizing operations and decision-making in areas like supply chain management and healthcare. The synergy of intelligent processing with security intelligence further paves the way for secure and intelligent systems.

This literature review identifies that the integration of AI with IoT is not only enabling new technological capabilities but also necessitates a focus on privacy and ethical considerations. The resulting advancements present a dual challenge of ensuring data security and upholding ethical standards in technology application. Understanding these trends and their implications is paramount for researchers and practitioners navigating the complex landscape of IoT-driven data analysis.

The integration of AI with the IoT is undergoing a significant transformation, driven by several key technological trends and advancements, as Edge AI and On-Device Learning, Federated Learning, Natural Language Processes Integration and AI-Driven Data Analytics.

Gaining increased traction, Edge AI and on-device learning are revolutionizing real-time decision-making and reducing reliance on cloud-based systems. This trend is evidenced by the

 doi:10.20944/preprints202312.2184.v1

development of Edge-IIoTset, a comprehensive cybersecurity dataset for IoT and IIoT applications [19,72].

The Federated Learning is emerging as a solution to privacy concerns, it enhances data security in IoT networks. It enables AI models to be trained across decentralized devices while keeping data localized, as illustrated in studies by Gu et al. [86].

On the other hand, Advancements in Deep Learning and Neural Networks are increasingly applied to process and analyze complex IoT data streams. They facilitate pattern recognition and predictive analytics, a trend highlighted by the research of Sipola et al. (Sipola et al., 2022). And Natural Language Processing (NLP) Integration is enabling more sophisticated user interactions through voice recognition and conversational AI. This development is transforming how users interact with IoT devices.

Collectively, these trends are contributing significantly to the evolution of AI in IoT, enabling the development of smarter, more efficient, and secure systems. The dynamic interplay of these technologies is not only redefining the capabilities of IoT devices but also paving the way for future innovations in this field.

There are a lot of Applications and Case Studies in bibliography, for example regarding to the integration of AI in IoT is significantly advancing smart home automation, optimizing energy management, and enhancing security systems. AI-powered devices like smart thermostats (e.g., Nest) are adapting to user preferences to optimize energy usage [86]. AI-enhanced security systems, such as Ring, employ facial recognition and anomaly detection to enhance home security [67]. Studies like that of Shikhli [69] and Saha [62] further underscore the sustainable impacts and holistic control afforded by smart home automation systems.

In healthcare, AI-driven IoT, particularly in wearable technologies, is revolutionizing remote patient monitoring and diagnostics. Wearable biosensors, integrated with AI, enable continuous health monitoring, as highlighted by Neumann et al. (Neumann, W.P. et al., 2023).

Furthermore, in the industrial sector, AI is transforming manufacturing processes through predictive maintenance. IoT sensors and AI algorithms are utilized to predict equipment failures, thus optimizing operational efficiency [73]. Hadi [25] illustrate the use of deep reinforcement learning in developing predictive maintenance models for effective resource management in industrial IoT.

AI is pivotal in IoT applications for environmental monitoring, aiding in climate change research and pollution control. AI algorithms analyze data from IoT environmental sensors to monitor air and water quality, contributing to sustainable resource management. Mehbodniya and Kant further demonstrate the application of IoT in environmental monitoring and control [32,44].

AI significantly influences urban environments and transportation systems. Smart traffic management systems, powered by AI, optimize traffic flow, and reduce congestion. The role of AI in autonomous vehicles is also crucial for enhancing safety and efficiency in transportation.

In conclusion, these applications and case studies collectively demonstrate AI's diverse and impactful role across various sectors in IoT. From transforming home environments and healthcare delivery to revolutionizing industrial operations and urban development, AI's integration with IoT is paving the way for innovative solutions and enhanced efficiencies.

5.2. Future prospect and challenges

The application of AI in IOT leads to some Technical Challenges. For example, 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, Zhao Wang et al. propose an AI-based cloud-edge-device collaboration framework optimized through task offloading algorithms [87,88]. Moreover, managing communication between diverse IoT devices demands advanced interoperability solutions capable of handling the complexity of data flows within these networks [34].

On 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

 doi:10.20944/preprints202312.2184.v1

methods and secure data transmission protocols [71]. Federated learning models introduce unique challenges, such as susceptibility to data poisoning and evasion attacks, necessitating stringent security measures [59]. 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 [88].

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 [36].

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 et al. demonstrate a dropout-tolerable federated learning scheme in healthcare, balancing privacy with effective [90]. Similarly, Loukil et al. 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. [39]

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. 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 [28,35].

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 [21].

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 advancement in wireless communication technologies, such as 5G and the upcoming 6G, have greatly enhanced the IoT systems' performance [33,55]. Vu Khanh et al. describe a visionary perception of IoT as the primary force driving digital revolution and mentions the challenges of existing common communication technologies in IoT systems [33]. Pattnaik et al. 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 (Pattnaik, S.K et al., 2022). 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 an insight into the technical evolution and future techniques to prolong the use of resources such as battery life [57]. 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 [11]. Bibri et al. explain that advanced ICT has significantly influenced the manifestation of

 doi:10.20944/preprints202312.2184.v1

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.

5.3. Limitations and Gaps in Current Research

Despite significant advancements in AI and IoT, there remain notable limitations and gaps in current research, well-documented in various studies. Taimoor and Rehman [74] 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 et al. [5] 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 [49] 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 et al. [17] 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 et al. 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 [8]. This review endeavors to bridge these gaps by integrating AI with IoT in practical applications, addressing the ethical considerations and future sustainability.

6. RQ answers and conclusions

The intersection between Artificial Intelligence (AI) and the Internet of Things (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 [58], credit risk evaluation innovation [10], and the automation strategy in smart cities [16]. This integration provides an enhanced customer experience and more informed business decisions through intelligent data analysis [58,60]. 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.

6.1. RQ1 - What are the latest emerging trends in integrating Artificial Intelligence (AI) with the Internet of Things (IoT)?

The emergent integration of Artificial Intelligence (AI) with the Internet of Things (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

 doi:10.20944/preprints202312.2184.v1

technologies to address the escalating complexity in today's data-driven healthcare sector [22,31,66]. For instance, the development of IoT-based systems like real-time respiratory rate monitoring through accelerometer sensors is aiding in remote patient monitoring [6]. In the application of patient-centric healthcare, IoMT is enhancing the scalability and effectiveness of healthcare delivery [22,66]. The study by Krishna Prasad Satamraju and B. Malarkodi, 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 Adeniyi Onasanya and M. Elshakankiri [52], 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 [23,70]. Sindhusaranya B. and colleagues discuss a federated learning and blockchain-enabled privacy-preserving system for fraud prevention and security in IoMT. A similar perspective is shared by L. Godlin Atlas and co-workers, showcasing a decentralized privacy-preserving blockchain for IoT and big data in healthcare applications. However, Brian Parker and C. Bach [54] 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 technologies are transforming healthcare by enabling high efficiency, advanced patient monitoring, and robust data security. However, as Brian Parker and C. Bach note, these advancements also demand careful considerations of the associated ethical, legal, and social implications to ensure responsible and sustainable use of technology.

6.2. RQ2 - How is intelligent data analysis transforming 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 Artificial Intelligence (AI) and the Internet of Things (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 [40]. Similarly, recent research outlines an intelligent technique for managing and analyzing network resources within a 5G-IoT-based smart healthcare network [82]. 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, Yaji et al. have demonstrated two encryption schemes, namely Goldwasser-Micali and Paillier, for preserving data privacy in AI applications implemented over blockchain [68]. 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 [63]. 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 [29]. 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.

 doi:10.20944/preprints202312.2184.v1

6.3. RQ3 - What challenges and opportunities does privacy protection present in AI-enhanced IoT?

Privacy and data protection in the Internet of things (IoT) and artificial intelligence (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 [58,61]. 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 privacy of healthcare data. For example, Healthchain was introduced as a scheme to ensure that both IoT data and doctors' diagnosis cannot be tampered with to avoid medical disputes, thereby enhancing the reliability of smart healthcare systems [61]. Other works discuss the pressing need for suitable regulatory frameworks and compliance issues within IoT devices relating to healthcare data privacy [58], and some even propose extending blockchain application 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 [37]. 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 [16]. 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 dissemination frameworks [60]. These carefully leverage blockchain principles within IoMT (Internet of Medical Things) 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-integrated 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.

6.4. RQ4 - How can AI contribute to more secure and private data management in IoT?

The contemporary discourse on the confluence of AI, Internet of Things (IoT), big data and blockchain technologies focalizes on the potentiality of these technologies in revolutionizing various domains, with particular emphasis on the healthcare sector. The pertinence of these technologies, particularly in relation to the protection and confidentiality of data therein, is markedly apparent. Omrčen et al. [51] provides an 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, and Sharma [30]. 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 et al. [14] 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 confidentiality, security, and privacy of healthcare data. In the context of AI's potential in revolutionizing healthcare delivery systems through the use of 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.

6.5. RQ5 - What are the ethical and social implications of using AI in IoT, particularly 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 [78], 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 transaction, 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 [45], 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 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 [78]. By ensuring the confidentiality and security of patient information, we can contribute to the development of innovative and smart healthcare systems that prioritize 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 development 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.

6.6. Conclusions

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. The development of such frameworks that use deep learning and blockchain to leverage intelligent data analysis and provide robust data security in 5G-enabled IoT systems, along with innovative solutions within the secure healthcare data dissemination domain, are crucial steps towards a more secure and efficient healthcare system. As we look to the future, it is important for research to delve further into amplifying these strategies and managing the potential risks involved in their implementation. The integration of AI with IoT, augmented by blockchain technology, can significantly enhance the privacy, security, and functionality of IoT within healthcare. Our aim is to contribute to the development of innovative and smart healthcare systems that prioritize security, privacy, and confidentiality of medical records, while addressing the potential ethical and social implications of these advanced technologies in healthcare and data privacy.

Moving forward, the comprehensive frameworks developed through our research will not only contribute to the ethical and responsible use of AI in IoT but also ensure the confidentiality and security of patient information, ultimately leading to the transformation of healthcare systems.

In summarizing, this paper has illuminated the transformative impact and challenges inherent in the AI-IoT nexus. It underscores the need for continuous innovation in addressing privacy, security, and ethical considerations, pivotal for the sustainable advancement of these technologies. The research calls for a balanced approach, integrating technological prowess with a strong ethical framework. As the AI-IoT landscape evolves, it is imperative for practitioners and policymakers to navigate these complexities with informed strategies, ensuring that the benefits of this integration are realized responsibly and effectively. The future of AI in IoT thus lies in harmonizing technological advancement with ethical integrity and privacy protection.

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. Aggarwal, N., & Singh, D.N. (2021). Technology assisted farming: Implications of IoT and AI. IOP Conference Series: Materials Science and Engineering, 1022.
2. Agarwal, K., Agarwal, K., Jha, A.K., & Joshi, I. (2022). Intelligence and Internet of Things with 5G Technology: Application and Development. *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, 762-766.
3. Al-Janabi, S. (2021). Overcoming the Main Challenges of Knowledge Discovery through Tendency to the Intelligent Data Analysis. *2021 International Conference on Data Analytics for Business and Industry (ICDABI)*, 286-294.
4. Aldboush, H.H., & Ferdous, M. (2023). 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*.
5. Aitlmoudden, O., Housni, M., Safeh, N., & Namir, A. (2023). A Microservices-based Framework for Scalable Data Analysis in Agriculture with IoT Integration. *International Journal of Interactive Mobile Technologies (iJIM)*.

6. Andarevi, M.H., & Iskandar, A.A. (2022). A Prototype of IoT-based Real-time Respiratory Rate Monitoring Using an Accelerometer Sensor. *2022 4th International Conference on Biomedical Engineering (IBIOMED)*, 42-46.
7. Aruna, S., Mohana Priya, S., Reshmeetha, K., Salai Sudhayini, E., & Ajay Narayanan, A. (2023). Blockchain Integration with Artificial Intelligence and Internet of Things Technologies. *2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 688-694.
8. Ataei Kachouei, M., Kaushik, A., & Ali, M.A. (2023). Internet of Things-Enabled Food and Plant Sensors to Empower Sustainability. *Advanced Intelligent Systems, 5*.
9. M. J. Baucas, P. Spachos and K. N. Plataniotis, "Federated Learning and Blockchain-Enabled Fog-IoT Platform for Wearables in Predictive Healthcare," in IEEE Transactions on Computational Social Systems, vol. 10, no. 4, pp. 1732-1741, Aug. 2023, doi: 10.1109/TCSS.2023.3235950.
10. Bi, W., & Liang, Y. (2022). Risk Assessment of Operator's Big Data Internet of Things Credit Financial Management Based on Machine Learning. *Mobile Information Systems*.
11. Bibri, S.E., Alexandre, A., Sharifi, A., & Krogstie, J. (2023). 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, 6*.
12. Borner, K., Scrivner, O., Cross, L.E., Gallant, M., Ma, S., Martin, A.S., Record, E.G., Yang, H., & Dilger, J.M. (2020). Mapping the co-evolution of artificial intelligence, robotics, and the internet of things over 20 years (1998-2017). *PLoS ONE, 15*.
13. Darwish, A.A., Hassanien, A.E., Elhoseny, M., Sangaiah, A.K., & Muhammad, K. (2019). 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, 10*, 4151-4166.
14. Dwivedi, S.K., Roy, P., Karda, C., Agrawal, S., & Amin, R. (2021). Blockchain-Based Internet of Things and Industrial IoT: A Comprehensive Survey. *Secur. Commun. Networks, 2021*, 7142048:1-7142048:21.
15. Elhoseny, M., Haseeb, K., Shah, A.A., Ahmad, I., Jan, Z., & Alghamdi, M.I. (2021). IoT Solution for AI-Enabled PRIVACY-PREServing with Big Data Transferring: An Application for Healthcare Using Blockchain. *Energies*.
16. Ezzat, M.A., Abd El Ghany, M.A., Almotairi, S., & Salem, M.A. (2021). Horizontal Review on Video Surveillance for Smart Cities: Edge Devices, Applications, Datasets, and Future Trends. *Sensors (Basel, Switzerland), 21*.
17. Faliagka, E., Panagiotou, C., Antonopoulos, C.D., Keramidas, G., & Voros, N.S. (2022). A Novel Marketplace Perspective Promoting Customized Low Energy Computing and IoT: The SMART4ALL Approach. *2022 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 363-368.
18. Fantin Irudaya Raj, E., Appadurai, M. (2022). Internet of Things-Based Smart Transportation System for Smart Cities. In: Mukherjee, S., Muppalaneni, N.B., Bhattacharya, S., Pradhan, A.K. (eds) Intelligent Systems for Social Good. Advanced Technologies and Societal Change. Springer, Singapore. https://doi.org/10.1007/978-981-19-0770-8_4
19. Ferrag, M.A., Friha, O., Hamouda, D., Maglaras, L.A., & Janicke, H. (2022). Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. *IEEE Access, PP*, 1-1.
20. Forbes, 2019 - The Fascinating Ways PepsiCo Uses Artificial Intelligence And Machine Learning To Deliver Success – https://www.forbes.com/sites/bernardmarr/2019/04/05/the-fascinating-ways-pepsico-uses-artificial-intelligence-and-machine-learning-to-deliver-success/?sh=5206c9ec311e
21. Gao, Y., Huang, Z., & He, J. (2023). Privacy-preserving and verifiable IoT data aggregation scheme based on blockchain and homomorphic encryption. *Other Conferences*.
22. Gomathi, L., Mishra, A.K., & Tyagi, A.K. (2023). Industry 5.0 for Healthcare 5.0: Opportunities, Challenges and Future Research Possibilities. *2023 7th International Conference on Trends in Electronics and Informatics (ICOEI)*, 204-213.
23. Godlin Atlas, L., Arjun, K.P., & Babu, B.S. (2021). A Decentralized Privacy-Preserving Blockchain for IoT and Big Data in Healthcare Applications. *Convergence of Blockchain, AI, and IoT*.
24. Gupta, N., Khosravy, M., Patel, N., Dey, N., Gupta, S., Darbari, H., & Crespo, R.G. (2020). Economic data analytic AI technique on IoT edge devices for health monitoring of agriculture machines. *Applied Intelligence*, 1-27.
25. Hadi, R.H., Hady, H.N., Hasan, A.M., Al-Jodah, A.A., & Humaidi, A.J. (2023). Improved Fault Classification for Predictive Maintenance in Industrial IoT Based on AutoML: A Case Study of Ball-Bearing Faults. *Processes*.
26. Ikharo, B.A., Obiagwu, A.E., Obasi, C., Hussein, S.U., & Akah, P. (2021). Security for Internet-of-Things Enabled E-Health using Blockchain and Artificial Intelligence: A Novel Integration Framework. *2021 1st International Conference on Multidisciplinary Engineering and Applied Science (ICMEAS)*, 1-4.
27. Jamil, F., Kahng, H., Kim, S., & Kim, D. (2021). Towards Secure Fitness Framework Based on IoT-Enabled Blockchain Network Integrated with Machine Learning Algorithms. *Sensors (Basel, Switzerland), 21*.

28. Javed, A.R., Hassan, M.A., Shahzad, F., Ahmed, W., Singh, S., Baker, T., & Gadekallu, T.R. (2022). Integration of Blockchain Technology and Federated Learning in Vehicular (IoT) Networks: A Comprehensive Survey. *Sensors (Basel, Switzerland), 22*.
29. Jiang, F., Chen, Z., Liu, L., & Wang, J. (2023). Federated Learning-Based Privacy Protection for IoT-based Smart Healthcare Systems. *2023 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, 1-6.
30. Jitendra Parmar, G.K. (2023). An Application of Blockchain: A Review. *Tuijin Jishu/Journal of Propulsion Technology*.
31. Junaid S.B., Imam A.A., Balogun A.O., De Silva L.C., Surakat Y.A., Kumar G., Abdulkarim M., Shuaibu A.N., Garba A., Sahalu Y., et al. Recent Advancements in Emerging Technologies for Healthcare Management Systems: A Survey. *Healthcare*. 2022; 10(10):1940. https://doi.org/10.3390/healthcare10101940
32. Kant, K., & Joshi (2023). Role of Modern technology in environmental monitoring and pollution control: An Analytical Study. *NeuroQuantology*.
33. Khanh, Q.V., Hoai, N.V., Manh, L.D., Le, A.N., & Jeon, G. (2022). Wireless Communication Technologies for IoT in 5G: Vision, Applications, and Challenges. *Wireless Communications and Mobile Computing*.
34. Lagkas, T.D., Argyriou, V., Bibi, S., & Sarigiannidis, P.G. (2018). UAV IoT Framework Views and Challenges: Towards Protecting Drones as "Things". *Sensors (Basel, Switzerland), 18*.
35. Lee, A.J., Biehl, J.T., & Curry, C. (2018). Sensing or Watching?: Balancing Utility and Privacy in Sensing Systems via Collection and Enforcement Mechanisms. *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*.
36. Liu, B., Zhang, X., Shi, R., Zhang, M., & Zhang, G. (2022). SEPSI: A Secure and Efficient Privacy-Preserving Set Intersection with Identity Authentication in IoT. *Mathematics*.
37. Liu, J., & Ren, W. (2022). 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*.
38. Liu, T.Y., & Wu, J. (2022). The Ethical and Societal Considerations for the Rise of Artificial Intelligence and Big Data in Ophthalmology. *Frontiers in Medicine, 9*.
39. Loukil, F., Ghedira, C., Boukadi, K., & Benharkat, A. (2021). Privacy-Preserving IoT Data Aggregation Based on Blockchain and Homomorphic Encryption. *Sensors (Basel, Switzerland), 21*.
40. Mani, V., Manickam, P., Alotaibi, Y., Alghamdi, S.A., & Khalaf, O.I. (2021). Hyperledger Healthchain: Patient-Centric IPFS-Based Storage of Health Records. *Electronics*.
41. Marengo, A., & Pagano, A. (2023). Investigating the Factors Influencing the Adoption of Blockchain Technology across Different Countries and Industries: A Systematic Literature Review. *Electronics*.
42. Market Research Future 2022 - https://www.marketresearchfuture.com/
43. Market Research Future 2023 - https://www.marketresearchfuture.com/
44. Mehbodniya, A., Haq, M.A., Kumar, A., Ismail, M.E., Dahiya, P., & Karupusamy, S. (2022). Data reinforcement control technique-based monitoring and controlling of environmental factors for IoT applications. *Arabian Journal of Geosciences, 15*.
45. Mochizuki, Y. (2019). AI and IoT for Social Value Creation. *2019 IEEE Asian Solid-State Circuits Conference (A-SSCC)*, 99-102.
46. Mukherjee, S., Gupta, S., Rawlley, O., & Jain, S. (2022). Leveraging big data analytics in 5G-enabled IoT and industrial IoT for the development of sustainable smart cities. *Transactions on Emerging Telecommunications Technologies, 33*.
47. Mukhopadhyay, S.C., Tyagi, S.K., Suryadevara, N.K., Piuri, V., Scotti, F., & Zeadally, S. (2021). Artificial Intelligence-Based Sensors for Next Generation IoT Applications: A Review. *IEEE Sensors Journal, 21*, 24920-24932.
48. Najim, A.H., Elkhediri, S., Alrashidi, M., & Nasri, N. (2022). The Impact of using IoT for Elderly and Disabled Peoples Healthcare: An Overview. *2022 2nd International Conference on Computing and Information Technology (ICCIT)*, 394-398.
49. Nishtar, Z., & Afzal, J. (2023). A Review of Real-Time Monitoring of Hybrid Energy Systems by Using Artificial Intelligence and IoT. *Pakistan Journal of Engineering and Technology*.
50. Nizam, H., Zafar, S., Lv, Z., Wang, F., & Hu, X. (2022). Real-Time Deep Anomaly Detection Framework for Multivariate Time-Series Data in Industrial IoT. *IEEE Sensors Journal, 22*, 22836-22849.
51. Omrčen, L., Leventić, H., Romić, K., & Galić, I. (2021). Integration of Blockchain and AI in EHR sharing: A survey. *2021 International Symposium ELMAR*, 155-160.
52. Onasanya, A., & Elshakankiri, M. (2018). Secured Cancer Care and Cloud Services in IoT/WSN Based Medical Systems. *SGIoT*.
53. Pal, D., & Joshi, S. (2023). AI, IoT and Robotics in Smart Farming: Current Applications and Future Potentials. *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, 1096-1101.

54. Parker, B., & Bach, C. (2020). Synthesis of Blockchain, Artificial Intelligence and Internet of Things. *European Journal of Engineering and Technology Research*.
55. Pattnaik, S.K., Samal, S.R., Bandopadhaya, S., Swain, K., Choudhury, S., Das, J.K., Mihovska, A.D., & Poulkov, V.K. (2022). 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 (Basel, Switzerland), 22*.
56. Pervaiz, A., Hussain, F., Israr, H., Tahir, M.A., Raja, F.R., Baloch, N.K., Ishmanov, F., & Zikria, Y.B. (2020). Incorporating Noise Robustness in Speech Command Recognition by Noise Augmentation of Training Data. *Sensors (Basel, Switzerland), 20*.
57. Popli, S., Jha, R.K., & Jain, S. (2021). Green IoT: A Short Survey on Technical Evolution & Techniques. *Wireless Personal Communications, 123*, 525 - 553.
58. Ramasamy, L.K., Khan, F., Shah, M., Prasad, B.V., Iwendi, C., & Biamba, C.N. (2022). Secure Smart Wearable Computing through Artificial Intelligence-Enabled Internet of Things and Cyber-Physical Systems for Health Monitoring. *Sensors (Basel, Switzerland), 22*.
59. Rahman, M.A., Rashid, M.M., Hossain, M.S., Hassanain, E., Alhamid, M.F., & Guizani, M. (2019). Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City. *IEEE Access, 7*, 18611-18621.
60. Reddy, B Koti. (2023). Latest trends and their adoptions in electrical power systems - an industrial perspective. Indonesian Journal of Electrical Engineering and Computer Science. 29. 8-14. 10.11591/ijeecs.v29.i1.pp8-14
61. Saadia, D. (2021). Integration of Cloud Computing, Big Data, Artificial Intelligence, and Internet of Things: Review and Open Research Issues. *Int. J. Web Based Learn. Teach. Technol., 16*, 10-17.
62. Saha, S., Eidmum, M.Z., Hemal, M.M., Khan, M.A., & Muiz, B. (2022). IOT BASED SMART HOME AUTOMATION AND MONITORING SYSTEM. *Khulna University Studies*.
63. Saha, R., Kumar, G., Rai, M.K., Thomas, R., & Lim, S. (2019). Privacy Ensured ${e}$ -Healthcare for Fog-Enhanced IoT Based Applications. *IEEE Access, 7*, 44536-44543.
64. Sakib, S.M., Fouda, M.M., Fadlullah, Z.M., & Nasser, N. (2020). Migrating Intelligence from Cloud to Ultra-Edge Smart IoT Sensor Based on Deep Learning: An Arrhythmia Monitoring Use-Case. *2020 International Wireless Communications and Mobile Computing (IWCMC)*, 595-600.
65. Santamato, V.R., Esposito, D., Tricase, C., Faccilongo, N., Marengo, A., & Pange, J. (2023). Assessment of Public Health Performance in Relation to Hospital Energy Demand, Socio-Economic Efficiency and Quality of Services: An Italian Case Study. *Communication Systems and Applications*.
66. Satamraju, K.P., & Malarkodi, B. (2022). A Secured Healthcare Model for Sensor Data Sharing With Integrated Emotional Intelligence. *IEEE Sensors Journal, 22*, 16306-16313.
67. Sepasgozar, S., David Bienvenido-Huertas, J., Shirowzhan, S., & Sargolzae, S. (2021). Introductory Chapter: Intelligence, Sustainable and Post-COVID-19 Resilience Built Environment: An Agenda for Future. IntechOpen. doi: 10.5772/intechopen.97100
68. Shahid, J., Ahmad, R., Kiani, A.K., Ahmad, T., Saeed, S., & Almuhaideb, A.M. (2022). Data Protection and Privacy of the Internet of Healthcare Things (IoHTs). *Applied Sciences*.
69. Shikhli, S., Shikhli, A.M., Jarndal, A.H., Alsyouf, I., & Cheaitou, A. (2022). Towards Sustainability in Buildings: a Case Study on the Impacts of Smart Home Automation Systems. *2022 Advances in Science and Engineering Technology International Conferences (ASET)*, 1-8.
70. Sindhusaranya B., Yamini R., Manimekalai Dr.M.A.P. and Geetha Dr.K. (2023). 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*.
71. Singh, P., & Deep Singh, K. (2023). Security and Privacy in Fog/Cloud-based IoT Systems for AI and Robotics. *EAI Endorsed Transactions on AI and Robotics*.
72. Sipola, T., Alatalo, J., Kokkonen, T., & Rantonen, M. (2022). Artificial Intelligence in the IoT Era: A Review of Edge AI Hardware and Software. *2022 31st Conference of Open Innovations Association (FRUCT)*, 320-331.
73. Subekti, S., Pranoto, H., Salmon, B., Yusuf, S.Q., Suyadiyanto, S., Ariyadi, A., & Hamid, A. (2020). Preventive maintenance of taper bearing using Arduino in the application of industry 4.0. *International Research Journal of Engineering, IT and Scientific Research, 6*, 1-14.
74. Taimoor, N., & Rehman, S. (2022). Reliable and Resilient AI and IoT-based Personalised Healthcare Services: A Survey. *IEEE Access, PP*, 1-1.
75. Taneja, M., Jalodia, N., Byabazaire, J., Davy, A., & Olariu, C. (2019). SmartHerd management: A microservices-based fog computing–assisted IoT platform towards data-driven smart dairy farming. *Software, 49*, 1055 - 1078.
76. Tsai, J.W., Huang, C., Chu, C.C., & Fan, G. (2023). The Smart Applications of ICT and IoT with AI Techniques in IMS Network. *2023 24st Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 290-293.

77. Uddin, M.S., Asaduzzaman, M., Farzana, R., Hasan, M.S., Rahman, M., & Allayear, S.M. (2019). Implementation of Smart Indoor Agriculture System and Predictive Analysis. *ICACDS*.
78. Veeramakali, T., Siva, R., Sivakumar, B., Mahesh, P.C., & Krishnaraj, N. (2021). An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. *The Journal of Supercomputing, 77*, 9576 - 9596.
79. Verma, S., Kawamoto, Y., Fadlullah, Z.M., Nishiyama, H., & Kato, N. (2017). A Survey on Network Methodologies for Real-Time Analytics of Massive IoT Data and Open Research Issues. *IEEE Communications Surveys & Tutorials, 19*, 1457-1477.
80. Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., & Yu, N. (2019). Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data. *IEEE Internet of Things Journal, 6*, 8770-8781.
81. Yang, X., Cao, D., Chen, J., Xiao, Z., & Daowd, A. (2020). AI and IoT-based collaborative business ecosystem: a case in Chinese fish farming industry. *Int. J. Technol. Manag., 82*, 151-171.
82. Yang, K., Shi, Y., Zhou, Y., Yang, Z., Fu, L., & Chen, W. (2020). Federated Machine Learning for Intelligent IoT via Reconfigurable Intelligent Surface. *IEEE Network, 34*, 16-22.
83. Yanlin Mou, (2022). The Innovative Development of Russian Modern Oil Painting under the Background of Internet of Things and Artificial Intelligence. Security and communication networks. https://doi.org/10.1155/2022/6110129
84. Yue W., Zhi T., Xin F., Yan H., Cameron N., Kai Z. (2022). Distributed Swarm Learning for Internet of Things at the Edge: Where Artificial Intelligence Meets Biological Intelligence. Cornell University Arxiv.org. https://doi.org/10.48550/arXiv.2210.16705
85. Yukitake, T. (2017). Innovative solutions toward future society with AI, Robotics, and IoT. *2017 Symposium on VLSI Circuits*, C16-C19.
86. Gu, B., Wang, Z., Zhou, Z., Mumtaz, S., Rodriguez, J., & Rodrigues, J.J. (2019). Intelligent Network Selection Mechanism in Macro-Femto HetNets Considering Network Connectivity and Users' Preference. *2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 1-5.
87. Wang, Y., Tian, Z., Fan, X., Huo, Y., Nowzari, C., & Zeng, K. (2022). Distributed Swarm Learning for Internet of Things at the Edge: Where Artificial Intelligence Meets Biological Intelligence.
88. Wang, Z., Zhou, Z., Zhang, H., Zhang, G., Ding, H., & Farouk, A. (2022). AI-Based Cloud-Edge-Device Collaboration in 6G Space-Air-Ground Integrated Power IoT. *IEEE Wireless Communications, 29*, 16-23.
89. Wei, W., Guizani, M., Ahmed, S.H., & Zhu, C. (2020). Guest Editorial: Special Section on Integration of Big Data and Artificial Intelligence for Internet of Things. *IEEE Transactions on Industrial Informatics, 16*, 2562-2565.
90. Zhang, L., Xu, J., Vijayakumar, P., Sharma, P.K., & Ghosh, U. (2023). Homomorphic Encryption-Based Privacy-Preserving Federated Learning in IoT-Enabled Healthcare System. *IEEE Transactions on Network Science and Engineering, 10*, 2864-2880.