Future Generation of Communication and Internet of Things (FGCIOT)

Journal homepage: http://fgciot.semnaniau.ac.ir/

Artificial Intelligence, Blockchain, and the Internet of Things in the Age of Machine Learning: Opportunities, Challenges, and Future Perspectives

***Alireza joshan*[1]**

[1]*Master of Science in Electrical Power Engineering, Faculty of Electrical Engineering, University of Guilan, Guilan, Iran.*

Article Info

Keywords:
Artificial Intelligence; Machine Learning; Blockchain; Internet of Things; Data Security; Smart City.

*Corresponding Author's Email Address:

Alireza.joshan.guilan@gmail.com

Abstract

The convergence of emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML), Blockchain, and the Internet of Things (IoT) has increasingly become a driving force behind technological advancements. This convergence facilitates the development of intelligent and autonomous systems across various domains such as supply chain management, smart cities, digital healthcare, and logistics, directly enhancing efficiency, decision-making, and system security. AI and ML, by analyzing big data and creating predictive algorithms, offer new capabilities for process optimization. On the other hand, IoT, by connecting devices and providing accurate, real-time data, enables fast and informed decision-making, while Blockchain offers enhanced security and transparency for data management and recording.

Despite the significant opportunities these technologies provide, challenges such as Blockchain scalability, IoT computational constraints, data privacy concerns, and the lack of standardized protocols for implementation remain prevalent. This paper comprehensively explores these opportunities and challenges, evaluating the latest research findings and offering solutions for overcoming barriers to successful implementation across various industries. Additionally, a roadmap for future research in this field is presented, emphasizing the need for the development of international standards to facilitate global collaboration and coordination.

Introduction

In the present era, the emergence of innovative digital technologies has always marked a turning point in industrial and societal transformations. One of the key technologies that has attracted significant attention in recent years is the Internet of Things (IoT). This technology, by connecting billions of devices and sensors to a global network, enables the generation of massive real-time data streams. These data, if not intelligently processed and analyzed, may remain meaningless and become a vast accumulation of useless information rather than creating value. Therefore, the use of advanced tools such as Machine Learning (ML) and Artificial Intelligence (AI) to process and analyze this data has become a fundamental need in IoT ecosystems. These tools enable automated decision-making, pattern prediction, and process optimization, ultimately leading to the creation of smart and autonomous systems that can operate effectively with minimal human intervention [1].

A fundamental challenge in IoT ecosystems is data security and trustworthiness. The data generated within these networks, due to their sensitivity and high value, must be managed in a way that prevents fraud, tampering, or loss of information. In this context, Blockchain, as a distributed and immutable ledger, offers an effective solution. Blockchain, by providing transparency, traceability, and data integrity, ensures the security of data within IoT ecosystems [2]. This technology, by establishing a decentralized and tamper-resistant system, can help safeguard the integrity of data on a global scale and protect processes from external vulnerabilities and risks.

The integration of AI, ML, IoT, and Blockchain can create autonomous and intelligent ecosystems where data is securely stored and processed, and decisions are made autonomously with minimal human intervention. Figure 1 is an infographic or concept image that shows how AI, ML, IoT, and Blockchain are merging to process data securely and intelligently. This convergence has shown

remarkable applications in various fields such as global supply chains [3], digital healthcare [4], intelligent transportation [5], and smart cities [6]. For instance, in global supply chains, these technologies can enable more precise tracking of goods, demand forecasting, and resource optimization. In healthcare, analyzing data produced by IoT devices and using ML algorithms can help predict diseases and assess patient conditions more quickly [7].

However, there are still limitations to the widespread implementation of these technologies. One such limitation is the scalability of public blockchains, which may be inadequate for processing the massive volumes of data generated by IoT devices [8]. Moreover, the computational constraints of IoT devices may prevent full utilization of the potential of these technologies, as many devices have limited processing power and cannot perform the complex computations needed for data analysis effectively. Additionally, regulatory and legal issues surrounding the protection of sensitive data, especially in sectors such as healthcare and banking, remain a significant obstacle to the widespread adoption of these technologies [9].

Given these challenges and opportunities, a comprehensive review of the current status, opportunities, and challenges of these converging technologies is essential. This paper provides a critical analysis of recent research, offering insights into the current state of the field and identifying future research directions. The research not only helps to better understand the synergy of these technologies but also paves the way for developing new, reliable models for their application across various industries[10-12].

Ultimately, the aim of this paper is to investigate the convergence of AI, ML, IoT, and Blockchain as an integrated solution that can accelerate digital transformation in various sectors and enhance efficiency, security, and service quality. Moreover, this paper seeks to address the existing limitations and challenges in this path and proposes solutions to overcome them in order to make these technologies more effective in different industries.

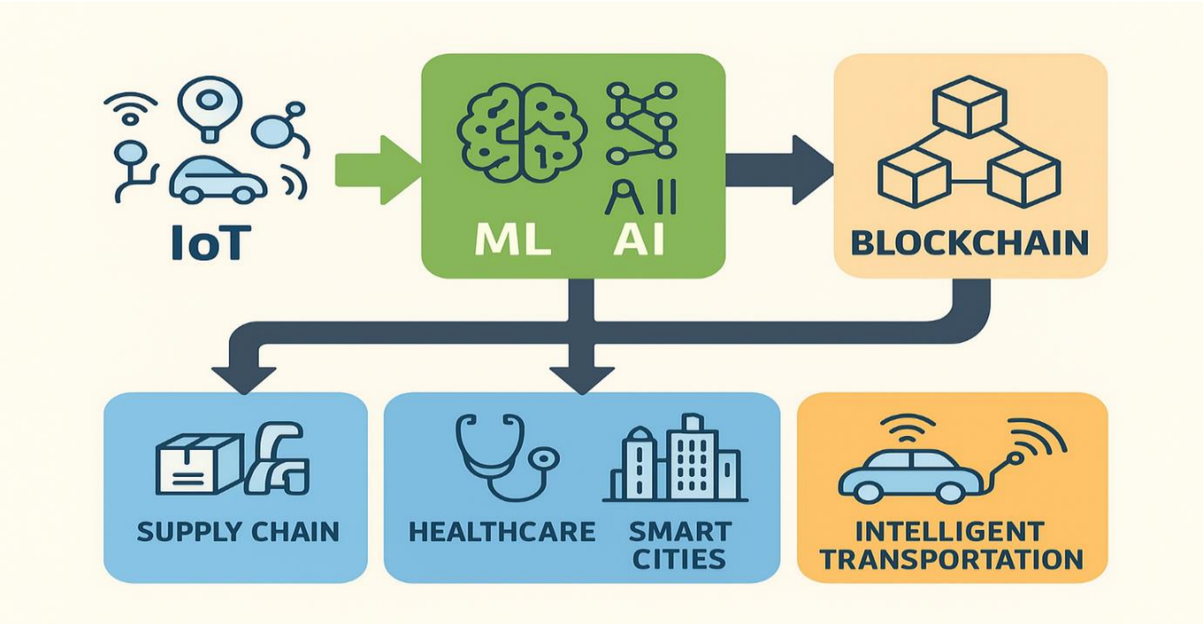

Fig.1: Integration of AI,ML,IoT,and Blochchain in smart Ecosystems

Background and Definitions

A. Artificial Intelligence (AI) and Machine Learning (ML)

Artificial Intelligence (AI) is the branch of computer science that aims to build systems capable of performing tasks that would typically require human intelligence, such as reasoning, problem-solving, pattern recognition, and autonomous decision-making [2]. Within AI, Machine Learning (ML) is a core discipline that enables systems to improve their performance by learning from data rather than relying solely on explicit programming. ML can be categorized into supervised learning, where models are trained on labeled datasets; unsupervised learning, which identifies hidden patterns in unlabeled data; and reinforcement learning, where agents learn optimal behaviors through interaction with an environment [3]. The combination of AI and ML provides the analytical and predictive power necessary to handle the massive and heterogeneous data streams generated by IoT devices.

Recent advances have made AI and ML indispensable in various fields. In healthcare, Google's AlphaFold system applied deep learning models to predict protein structures with near-experimental accuracy, enabling breakthroughs in biomedical research [12]. In smart cities, ML algorithms have been deployed to process IoT sensor data for traffic management. For instance, the city of Hangzhou in China implemented an AI-driven traffic optimization system that reduced congestion levels by over 15% by dynamically adjusting traffic signals based on real-time conditions [13]. In agriculture, ML has been combined with IoT soil sensors to predict soil quality and optimize irrigation schedules, leading to higher yields with reduced water consumption [15]. These examples highlight that AI and ML not only provide the capability to analyze big data but also translate such analysis into actionable decisions that directly impact efficiency, cost reduction, and sustainability.

B. Blockchain Technology

Blockchain is a distributed ledger technology (DLT) that records transactions across decentralized networks of computers, ensuring transparency, immutability, and tamper resistance [3]. Unlike traditional centralized databases controlled by a single authority, blockchain relies on consensus mechanisms such as Proof-of-Work (PoW) or Proof-of-Stake (PoS) to validate transactions, making it highly secure and resistant to fraud. Each transaction is cryptographically linked to the previous one, forming a continuous chain of blocks, hence the name blockchain.

Beyond its initial use in cryptocurrencies such as Bitcoin, blockchain has found widespread applications across industries. In supply chain management, Walmart and IBM collaborated on the Food Trust Blockchain to track agricultural products from farms to retail shelves, reducing the time to trace contaminated food from seven days to only 2.2 seconds [14]. In healthcare, MIT's MedRec project employed blockchain to manage electronic medical records, ensuring secure data exchange between patients and healthcare providers while maintaining transparency and accountability [15]. In governance and identity management, the European Blockchain Services Infrastructure (EBSI) initiative, supported by the European Commission, aims to develop cross-border blockchain-based public services, including secure digital identities [6,16].

Nevertheless, blockchain faces major challenges, particularly in scalability and energy consumption. Public blockchains such as Bitcoin and Ethereum suffer from low transaction throughput and high latency, making them less suitable for high-volume IoT data [9]. Energy-intensive consensus mechanisms, such as PoW, also raise environmental sustainability concerns, leading to ongoing research into more efficient alternatives such as Proof-of-Authority (PoA) and Proof-of-History (PoH). Despite these limitations, blockchain remains a cornerstone for building trust in decentralized IoT systems.

C. Internet of Things (IoT)

The Internet of Things (IoT) is a network of interconnected physical objects embedded with sensors, processors, and communication technologies that enable them to collect and exchange real-time data [1]. By bridging the physical and digital worlds, IoT empowers industries to monitor environments, automate operations, and provide context-aware services. Applications of IoT span across smart cities, industrial automation, healthcare, agriculture, and logistics, making it a foundational component of Industry 4.0.

Real-world deployments demonstrate IoT's transformative potential. In urban environments, Barcelona implemented an IoT-based smart city platform to optimize waste collection, monitor air quality, and manage parking systems, leading to significant improvements in service efficiency and environmental sustainability [17]. In healthcare, wearable IoT devices such as Fitbit and Apple Watch continuously collect patient vital signs and transmit them to medical platforms for preventive monitoring, while during the COVID-19 pandemic, IoT-enabled telehealth solutions facilitated remote diagnosis and treatment [4,18]. In industrial manufacturing, Siemens developed its MindSphere IoT platform to connect machines and equipment, enabling predictive maintenance and minimizing downtime [19,23].

However, IoT also introduces significant challenges. Devices are often resource-constrained in terms of computational capacity, memory, and battery life [10]. This makes it difficult to implement strong security mechanisms, leaving IoT networks vulnerable to cyberattacks such as distributed denial-of-service (DDoS) or unauthorized access. Additionally, the heterogeneity of IoT devices complicates interoperability, while the lack of unified global standards further limits large-scale deployment. These limitations make the integration of AI for intelligent processing and blockchain for secure communication critical to IoT's future success.

D. Convergence of AI, ML, Blockchain, and IoT

While AI, ML, blockchain, and IoT each deliver transformative benefits individually, their convergence produces synergistic ecosystems that are secure, intelligent, and autonomous. AI and ML bring intelligence by analyzing IoT-generated data and making predictive or prescriptive decisions. Blockchain ensures that this data is secure, immutable, and transparently shared across networks. IoT provides the data-generating backbone that fuels the entire ecosystem.

Practical implementations illustrate this convergence. In intelligent transportation systems, IoT sensors embedded in vehicles and infrastructure collect traffic and environmental data; ML algorithms process this information for route optimization and congestion reduction; and blockchain secures the communication between vehicles and control centers to prevent data tampering [7]. In supply chains, IoT devices track shipments in real time, ML models forecast demand and optimize inventory management, and blockchain guarantees product authenticity and traceability [5]. In healthcare, wearable IoT sensors monitor patient health continuously, ML models analyze these signals to detect early signs of disease, and blockchain ensures that sensitive patient data remains private and accessible only to authorized stakeholders [6]. Cutting-edge projects have begun experimenting with federated learning combined with blockchain, where ML models are trained across decentralized IoT nodes without centralizing raw data, thereby protecting privacy while enabling collective intelligence [20,22,43]. These examples highlight that the convergence of the four technologies has the potential to create truly autonomous, secure, and adaptive digital ecosystems Which is shown in Figure 2.

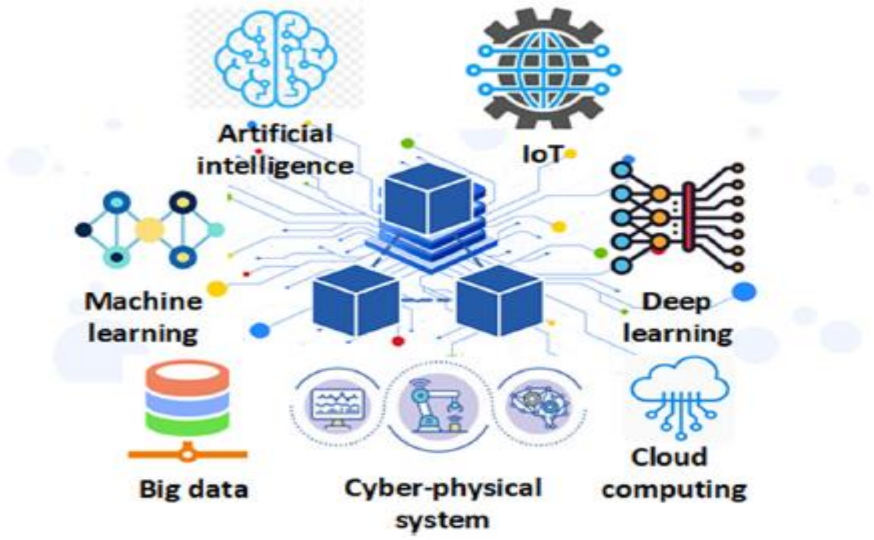

Fig.2: Convergence of blockchain, IoT, Artificial Intelligence, and other digital technologies

In summary, AI and ML provide the analytical intelligence to transform raw IoT data into meaningful insights, blockchain guarantees the security and trustworthiness of digital interactions, and IoT serves as the data-generating infrastructure that connects the physical and digital worlds. Their convergence marks a paradigm shift in digital transformation, opening opportunities in domains such as supply chains, healthcare, transportation, and smart cities. However, the challenges of scalability, security, and interoperability highlight the need for continued research and innovation. The next section describes the methodology used in this review to systematically examine the applications, challenges, and opportunities arising from these converging technologies.

Research Methodology

This study adopts a systematic review methodology to provide a comprehensive understanding of the convergence of AI, ML, IoT, and blockchain technologies. The methodology consists of the following steps:

A. Literature Search

A systematic search of academic databases was conducted, including IEEE Xplore, ScienceDirect, SpringerLink, MDPI, and Frontiers. The search strategy involved combinations of keywords such as:

A. "Artificial Intelligence AND Blockchain AND IoT"
B. Machine Learning AND IoT AND Blockchain"
C. "AI AND Smart Cities AND IoT"
D. "Digital Healthcare AND Blockchain AND ML"

The search was limited to peer-reviewed journal articles and conference papers published between 2017 and 2025 to ensure the inclusion of recent advancements.

B. Inclusion and Exclusion Criteria

To maintain quality and relevance, the following inclusion criteria were applied:

A. Focus on at least two converging technologies among AI, ML, IoT, and blockchain.
B. Clearly defined applications, challenges, or opportunities in real-world or simulated environments.
C. High citation impact or publication in reputable journals or IEEE conferences.

Exclusion criteria included:

A. Studies lacking technical depth or empirical evidence.
B. Non-English publications.
C. Duplicate studies reporting the same dataset without additional insights.

C. Data Extraction and Categorization

After filtering, the selected studies were thoroughly reviewed, and the following data were extracted:

A. Authors, year of publication, and country of study.
B. Technologies involved and their combination.

C. Application domain (e.g., supply chain, smart cities, healthcare, transportation).

D. Identified challenges and proposed solutions.

E. Methodology used (simulation, case study, or field deployment).

The extracted data were then categorized into three main domains:

A. Applications – highlighting use cases and benefits of technology convergence.

B. Challenges – addressing technical, security, privacy, and standardization issues.

C. Opportunities and Future Directions – identifying research gaps and potential advancements.

D. Analysis Approach

A qualitative synthesis was conducted, focusing on trends, patterns, and critical gaps in the existing literature. The narrative approach allowed for the integration of heterogeneous studies, including conceptual, simulation-based, and empirical research, providing a holistic view of the current state of AI, ML, IoT, and blockchain convergence.

The analysis also involved comparative evaluation using tables to illustrate applications, challenges, and research status, allowing clear visualization of trends and identifying areas for further research.

Applications and Challenges of Technology Convergence

The convergence of innovative technologies such as the Internet of Things (IoT), Machine Learning (ML), Artificial Intelligence (AI), and Blockchain has created immense potential in various industrial and societal domains. By integrating these technologies, organizations are able to enhance their operations, improve efficiency, and create new value. However, while the opportunities are evident, many of the current applications remain at the pilot or conceptual stage, and several fundamental challenges limit large-scale adoption [13,14]. In this context, some of the key applications of this convergence are examined, along with a critical discussion of the challenges that must be overcome for their optimal utilization, as illustrated in Figure 3.

In the field of Global Supply Chains, the integration of IoT, Blockchain, and ML has significantly optimized processes. Blockchain ensures the authenticity of products by creating a distributed and immutable ledger, preventing fraud and counterfeiting [13]. IoT serves as a tool for real-time tracking of goods, where sensors can monitor conditions such as temperature and humidity during transportation [14]. ML algorithms provide demand forecasting, supporting more efficient inventory management and reducing shortages and overstocking [15]. Although these applications highlight clear advantages, practical deployment faces barriers such as Blockchain scalability and high transaction costs. The root cause lies in consensus mechanisms like Proof-of-Work, which limit throughput and energy efficiency. Solutions such as Proof-of-Stake and sharding have been proposed, but evidence from real-world implementations remains scarce [27].

In Digital Healthcare, IoT sensors can continuously collect patient data, supporting early diagnosis or disease prevention [16]. ML algorithms analyze this data to predict health conditions, while Blockchain secures sensitive medical records and prevents unauthorized access [17]. Projects like Healthereum demonstrate the feasibility of this convergence [18]. Yet, privacy protection and legal compliance remain unresolved challenges. Although methods such as homomorphic encryption and permissioned Blockchains have been suggested, they introduce high computational overhead and lack harmonized international regulations [29]. This indicates that legal and ethical frameworks, rather than technology itself, are the primary barriers in this domain.

In the domain of Smart Cities, AI analyzes large-scale data (e.g., from cameras, sensors, and social media) to simulate and predict urban trends [19]. IoT supports intelligent resource management in areas such as water and energy [20], while Blockchain ensures secure and transparent handling of public and financial data [21]. Barcelona's data exchange initiative demonstrates practical progress [22]. However, these projects often remain city-specific and fragmented. The lack of global standards and interoperability frameworks makes replication at scale difficult, limiting broader impact [31].

In Intelligent Transportation, IoT, AI, ML, and Blockchain contribute to route optimization, fleet management, and secure data exchange. Autonomous vehicles rely on AI for decision-making [23], ML for traffic prediction [24], IoT for V2V and V2I communication [25], and Blockchain for securing transport-related data [26]. Despite their promise, cybersecurity threats and the scarcity of extensive field experiments highlight a gap between theoretical models and practical deployment [30]. Lightweight Blockchain designs have been proposed to address latency and security, but large-scale validation remains limited.

However, the convergence of these technologies faces several challenges that must be addressed for effective implementation. One of the main challenges is Blockchain scalability. Public Blockchain systems such as Bitcoin and Ethereum suffer from low transaction throughput and high energy consumption, which hinder their widespread adoption in IoT-based applications [27]. Additionally, the resource constraints of IoT devices, such as limited computational power and battery life, restrict the execution of complex ML and AI algorithms locally on these devices [28]. Furthermore, data privacy and security concerns, especially regarding sensitive and personal data, remain a significant challenge [29]. While Blockchain can enhance data security, its transparency can itself become problematic for sensitive applications, and numerous cybersecurity threats must still be mitigated [30]. Lastly, the lack of global standards has resulted in fragmented technical and regulatory frameworks across different countries, creating barriers for large-scale, international implementations [31]. Establishing unified standards and regulations is essential to streamline and expand adoption [32].

Fig.3: Smart applications of proposed conceptual framework based on blockchain, IoT, Artificial Intelligence,and other digital technologies

Findings and Critical Analysis

Analysis of the literature reveals several key observations regarding the convergence of IoT, ML, AI, and Blockchain:

A. Single-dimensional focus: Many studies focus on combinations of only two technologies (e.g., IoT + Blockchain), while comprehensive four-technology integration remains limited [33,35]. This limitation suggests that current research often overlooks potential synergies among all four technologies, which may restrict the discovery of more effective solutions in complex industrial and societal applications.

B. Lack of field experiments: Most research is conceptual or simulation-based, with limited real-world deployment [37]. This gap indicates that although theoretical models show potential, practical challenges such as system scalability, device constraints, and cybersecurity risks are not fully addressed. Consequently, the effectiveness and feasibility of proposed approaches remain uncertain when applied in real environments.

C. Standardization issues: The absence of unified protocols reduces interoperability across platforms [38]. While some frameworks have been proposed, they are often limited to specific domains or pilot projects. This fragmentation can prevent large-scale integration and slows the adoption of converged technologies across industries and regions.

D. Ethical and legal challenges: Storing sensitive medical or personal data on Blockchain requires robust legal frameworks [34]. Current studies highlight privacy-preserving methods, but they often increase computational complexity and do not fully resolve cross-border legal compliance issues. This indicates that addressing ethical and regulatory concerns is as critical as technological development.

Table 1: Comparative Analysis of Studies

Domain	Opportunities	Challenges	Research Status	Sample References
Supply Chain	Transparency, product tracking, demand prediction	Blockchain scalability	Advanced simulations	[33], [37]
Digital Healthcare	Data confidentiality, ML analytics	Privacy, legal issues	Predominantly theoretical	[34]
Smart Cities	Data analytics, resource sustainability	Standardization	Limited pilot studies	[36], [38]
Intelligent Transportation	Route optimization, cost reduction	Scalability, security	Limited field tests	[35], [37]

While the table summarizes existing research, a deeper analysis shows that most studies do not examine the root causes of challenges. For example, Blockchain scalability issues in supply chains stem from consensus mechanisms, while privacy challenges in digital healthcare often arise from inadequate regulatory harmonization. Moreover, ethical and legal concerns are rarely integrated into experimental designs, leaving gaps between theoretical potential and practical application. Addressing these gaps will require multi-dimensional studies that test full-scale integration, consider standardization frameworks, and incorporate ethical and legal compliance mechanisms alongside technological development.

A. Comparative analysis and motivational insights

Our study demonstrates several distinctive strengths compared to existing research in the domains of IoT, blockchain, and artificial intelligence. For instance, while certain works such as [44] examine the potential benefits and challenges of integrating blockchain and AI within IoT, our research goes further by offering a thorough analysis of specific synergies and presenting concrete solutions to address the identified challenges. Moreover, whereas studies like [45] primarily focus on security issues using machine learning, AI, and blockchain technologies, our contribution is distinguished by an in-depth examination of standardized security protocols and advanced cryptographic methods.

Another key contribution of our work lies in its comprehensive analysis of interoperability. Unlike prior research such as [46], which emphasizes general technical challenges, we propose frameworks that enable smoother integration between these technologies. Furthermore, we advance practical solutions to overcome the limitations of scalability, including scalable blockchain architectures specifically tailored for IoT.

While the review presented in [48] provides a comprehensive taxonomy and discussion of the challenges and opportunities associated with integrating blockchain and decentralized AI for cybersecurity, our study moves beyond this by proposing tangible solutions to both scalability and security concerns, as well as policy recommendations for the responsible deployment of these technologies.

Importantly, our analysis is not restricted to a single domain; instead, it extends across multiple sectors, thereby enhancing the breadth and applicability of our findings.

Table 2: List of related review works

Contribution	Topic of review	Year	Reference
Explores how blockchain and AI can be used to improve the performance of IoT systems. Focuses on the potential benefits, limitations, challenges, and future research directions in this emerging field.	Integration of blockchain and AI in the IoT	2023	[44]
Addresses security challenges in IoT through systematic study of ML, AI, and BCT technologies.	Security challenges and solutions in IoT: A review of ML, AI, and blockchain integration	2020	[45]
Provides a comprehensive overview of the convergence of IoT with blockchain and ML	Convergence of IoT with blockchain and ML: Overview and challenges	2024	[46]

algorithms, addressing technical challenges such as architecture, hardware, privacy and security, scalability, interoperability, and heterogeneity issues.			
Conducts a review of the integration of edge computing and blockchain into IoT systems, covering aspects of system architectures, categories of blockchain-based edge deployment, security requirements, and potential applications. Discusses challenges and insights into the future directions of blockchain-based edge IoT systems.	Integration of edge computing and blockchain into IoT: Challenges and opportunities	2024	[47]
Offers a systematic literature review on the integration of BCT with decentralized AI within cybersecurity, providing a comprehensive taxonomy, analyzing the challenges and opportunities, and discussing real-world applications and future research directions.	Integration of blockchain with decentralized AI for cybersecurity: A systematic literature review	2024	[48]
Discusses the potential of integrating advanced technologies to improve diagnostic accuracy and treatment efficacy in colorectal cancer care, emphasizing the importance of a multidisciplinary approach in healthcare innovations.	Integration of AI, IoT, Blockchain, and Nanotechnology in Colorectal Cancer Diagnosis and Treatment	2024	[49]
Reviews how these technologies can enhance efficiency, transparency, and security in logistics operations, providing insights into their collaborative potential for optimizing supply chain management.	Application of Blockchain, IoT, and AI in Logistics and Transportation	2024	[50]
Identifies key barriers to the adoption of these technologies in the construction sector and proposes strategic solutions to facilitate their integration, thereby enhancing project management and operational efficiency.	Challenges and Solutions for Implementing AI, IoT, and Blockchain in Construction	2023	[51]

Discusses the innovative approach of using federated learning combined with blockchain to bolster security measures in IoT systems, addressing vulnerabilities while ensuring data privacy and integrity.	Blockchain-Federated Learning for Enhancing IoT Security	2024	[52]

In contrast to reviews that concentrate exclusively on individual sectors such as logistics [50], construction [51], or colorectal cancer treatment [49], our study introduces integrated and standardized frameworks designed to be applicable across diverse industries. Within this context, we identify critical challenges in scalability and data management, and put forward targeted solutions to effectively address these issues.

Moreover, our research extends beyond the scope of existing reviews (e.g., [52]) by not only discussing the challenges but also offering concrete solutions and policy recommendations. Specifically, we emphasize scalability and security through the integration of advanced cryptographic techniques and robust data privacy frameworks. This comprehensive approach supports both the responsible deployment and the innovative advancement of IoT, blockchain, and AI technologies.

Roadmap for Future Research and Implementation

The convergence of Artificial Intelligence (AI), Machine Learning (ML), Blockchain, and the Internet of Things (IoT) is still in its formative stage. While numerous theoretical frameworks and pilot projects have demonstrated the potential of these technologies, large-scale deployment requires a clear roadmap that addresses technical, regulatory, and societal challenges. This section proposes a research and implementation roadmap divided into short-term, medium-term, and long-term priorities.

A. Short-Term Priorities (1–3 years)

In the short term, research should focus on overcoming the most immediate barriers that hinder real-world deployment. First, lightweight AI/ML algorithms must be developed to operate effectively on resource-constrained IoT devices, enabling on-device analytics and reducing reliance on cloud computing [39-42]. Second, energy-efficient blockchain protocols such as Proof-of-Authority (PoA) and Proof-of-History (PoH) should replace energy-intensive consensus models to support scalability and environmental sustainability. Third, interoperability standards need to be established to facilitate seamless communication among heterogeneous IoT devices and blockchain platforms. These initiatives are expected to accelerate the transition from conceptual studies to small-scale pilot implementations in sectors such as healthcare monitoring, intelligent transportation, and smart grid management.

B. Medium-Term Priorities (3–7 years)

Over the medium term, the focus should shift toward integrating these technologies into cross-domain ecosystems. For example, smart city platforms could simultaneously manage healthcare, transportation, and energy infrastructure using convergent AI–IoT–Blockchain architectures. At this stage, federated learning combined with blockchain is anticipated to play a crucial role in preserving data privacy while enabling collaborative AI model training across distributed IoT nodes. Additionally, legal and ethical frameworks must be established to govern the storage and exchange of sensitive data, particularly in sectors such as healthcare and finance. Regulatory sandboxes at the national and regional levels could support experimentation while ensuring compliance with emerging standards. Pilot studies should evolve into larger-scale deployments across metropolitan regions, supported by public–private partnerships.

C. Long-Term Priorities (7–15 years)

In the long term, the goal is the creation of fully autonomous and adaptive ecosystems where AI, ML, Blockchain, and IoT operate seamlessly at global scale. These ecosystems will leverage self-learning AI models embedded in IoT devices, quantum-safe blockchain protocols to ensure resilience against advances in quantum computing, and globally harmonized regulatory frameworks. Smart cities may evolve into cognitive cities, where real-time AI-driven decision-making governs transportation, healthcare, energy, and governance systems simultaneously. At this stage, the focus should also include sustainability considerations, ensuring that technological integration aligns with global goals such as carbon neutrality and equitable digital access.

Table 3: Roadmap Summary Table

Timeframe	Research & Technical Priorities	Industrial/Practical Focus	Expected Outcomes
Short-Term (1–3 yrs)	Lightweight ML for IoT; Energy-efficient blockchain protocols; Interoperability standards	Small-scale pilots in healthcare, transportation, smart grids	Feasibility studies; validated prototypes
Medium-Term (3–7 yrs)	Cross-domain integration; Federated learning with blockchain; Legal & ethical frameworks	City-level smart systems; national regulatory sandboxes	Regional deployment; privacy-preserving AI ecosystems
Long-Term (7–15 yrs)	Fully autonomous ecosystems; Quantum-safe blockchain; Global interoperability standards	Cognitive cities; industrial-scale automation	Global-scale adoption; sustainable and adaptive digital ecosystems

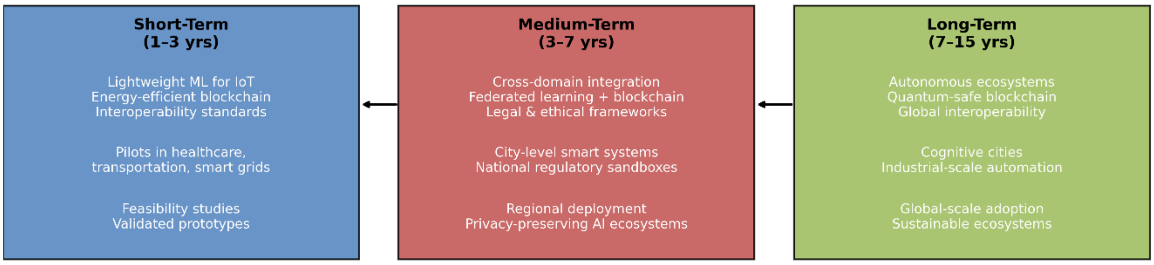

Fig.4: Research and Implementation Roadmap

Conclusion

A comprehensive examination of the convergence between Artificial Intelligence (AI), Machine Learning (ML), the Internet of Things (IoT), and blockchain technologies demonstrates that this integration holds the capacity to generate profound transformations across diverse sectors. The combined application of these technologies in areas such as supply chain transparency, healthcare data security, urban resource management, and transportation optimization can lead to significant improvements in system efficiency, security, and autonomy. These advancements not only enhance operational productivity but also contribute meaningfully to improving the overall quality of life.

Nonetheless, realizing the full potential of this technological synergy requires addressing several critical challenges. Among the most pressing are the scalability limitations of blockchain, primarily due to restricted transaction throughput and high energy consumption. Likewise, the limited computational resources and hardware constraints of IoT devices hinder the deployment of complex machine learning algorithms. Beyond technical barriers, the absence of universally adopted international standards, along with persistent concerns regarding legal frameworks and data privacy, pose significant obstacles that call for coordinated, cross-border collaboration.

Overcoming these challenges necessitates parallel efforts in both technological innovation and policy development. On the technological front, the creation of lightweight and resource-efficient machine learning algorithms tailored to the limitations of IoT devices, along with the design of energy-efficient and scalable consensus protocols for blockchain systems, are essential priorities. Simultaneously, from a policy perspective, the establishment of comprehensive international legal frameworks to ensure robust data privacy and cybersecurity alongside the development of globally accepted standards will be key to enabling the sustainable and responsible deployment of these technologies. Moreover, given that current research in these domains is still predominantly theoretical and reliant on simulations, there is a pressing need to conduct real-world field studies and urban pilot projects to evaluate practical feasibility and uncover real-life implementation challenges.

In this context, future research and development must focus on several strategic directions. First, machine learning algorithms should be optimized to operate efficiently within the resource-constrained environments of IoT devices. Second, blockchain consensus mechanisms need to evolve to become more scalable and energy-efficient, thus overcoming current performance bottlenecks. Third, robust international legal and regulatory frameworks must be developed to safeguard data privacy and facilitate cross-jurisdictional cooperation and trust. Finally, practical experimentation through urban-scale pilot programs and field deployments should be prioritized over exclusive reliance on simulated models, ensuring that technological solutions are grounded in real-world applicability.

By integrating these technological and policy-oriented approaches, the path can be paved for the widespread, effective, and sustainable adoption of AI, ML, IoT, and blockchain technologies ultimately enabling the development of intelligent, secure, and resilient systems at a global scale.

Table 4. Summary of Conclusions

Aspect	Key Findings	Future Recommendations
Applications	Supply chains, healthcare, smart cities, transportation	Expand real-world pilot studies
Challenges	Scalability, security, standardization	Develop new protocols and standards
Opportunities	Transparency, trust, optimization	Apply in industrial and urban scale
Research	Mostly theoretical and simulation-based	Conduct integrative and practical studies

Author Contributions

A. Joshan, collected the data, carried out the data analysis and interpreted the results and wrote the manuscript.

Acknowledgment

The author gratefully acknowledges the reviewer and editors of this journal.

Conflict of Interest

The author declares that there is no conflict of interests regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancies have been completely observed by the authors.

References

[1] H. El Hailouch, H. Saati, H. Nhaila, M. El Khaili, and H. E. Chakir, "Study of the Roles of IoT in the Transformation of Supplier Relationships in Industry 4.0," in 2025 5th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), May 2025, pp. 1-7, https://doi.org/10.1109/IRASET64571.2025.11008138

[2] G. B. Raja, "Impact of internet of things, artificial intelligence, and blockchain technology in Industry 4.0," in Internet of Things, Artificial Intelligence and Blockchain Technology, Cham: Springer International Publishing, 2021, pp. 157-178, https://doi.org/10.1007/978-3-030-74150-1_8

[3] Y. Lu, "The current status and developing trends of industry 4.0: A review," Information Systems Frontiers, vol. 27, no. 1, pp. 215-234, 2025, https://doi.org/10.1007/s10796-021-10221-w

[4] A. Singh, N. Kumar, M. Singh Kaswan, V. Kumar, and R. Chaudhary, "Industry 4.0 technologies and healthcare: a review of the current landscape and future prospects," International Journal of Industrial Engineering and Operations Management, 2025, https://doi.org/10.1108/IJIEOM-01-2025-0001

[5] Z. K. Idrissi, M. Lachgar, and H. Hrimech, "Blockchain, IoT and AI in logistics and transportation: A systematic review," Transport Economics and Management, vol. 2, pp. 275-285, 2024, https://doi.org/10.1016/j.team.2024.09.002

[6] A. Visvizi, R. Malik, G. M. Guazzo, and V. Çekani, "The Industry 5.0 (I50) paradigm, blockchain-based applications and the smart city," European Journal of Innovation Management, vol. 28, no. 1, pp. 5-26, 2025, https://doi.org/10.1108/EJIM-09-2023-0826

[7] N. Adamashvili, N. Zhizhilashvili, and C. Tricase, "The integration of the internet of things, artificial intelligence, and blockchain technology for advancing the wine supply chain," Computers, vol. 13, no. 3, p. 72, 2024, https://doi.org/10.3390/computers13030072

[8] Z. Balani and M. S. Mohammed, "The Convergence of AI and Blockchain Technologies: A Review on Enhancing IoT Security," in 2025 5th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), May 2025, pp. 1-7, https://doi.org/10.1109/IRASET64571.2025.11008214

[9] A. Kumar, S. K. Mangla, and P. Kumar, "Barriers for adoption of Industry 4.0 in sustainable food supply chain: a circular economy perspective," International Journal of Productivity and Performance Management, vol. 73, no. 2, pp. 385-411, 2024, https://doi.org/10.1108/IJPPM-12-2020-0695

[10] A. Alanhdi and L. Toka, "A survey on integrating edge computing with ai and blockchain in maritime domain, aerial systems, iot, and industry 4.0," IEEE Access, vol. 12, pp. 28684-28709, 2024, https://doi.org/10.1109/ACCESS.2024.3367118

[11] O. Kuznetsov, P. Sernani, L. Romeo, E. Frontoni, and A. Mancini, "On the integration of artificial intelligence and blockchain technology: a perspective about security," IEEE Access, vol. 12, pp. 3881-3897, 2024, https://doi.org/10.1109/ACCESS.2023.3349019

[12] R. Pant et al., "A systematic review of additive manufacturing solutions using machine learning, internet of things, big data, digital twins and blockchain technologies: a technological perspective towards sustainability," Archives of Computational Methods in Engineering, vol. 31, no. 8, pp. 4601-4616, 2024, https://doi.org/10.1007/s11831-024-10116-4

[13] N. Choi and H. Kim, "Technological Convergence of Blockchain and Artificial Intelligence: A Review and Challenges," Electronics, vol. 14, no. 1, p. 84, 2024, https://doi.org/10.3390/electronics14010084

[14] V. Vijaykumar, P. Mercy, T. Lucia Agnes Beena, H. M. Leena, and C. Savarimuthu, "Convergence of IoT, artificial intelligence and blockchain approaches for supply chain management," in Blockchain, IoT, and AI Technologies for Supply Chain Management: Apply Emerging Technologies to Address and Improve Supply Chain Management, Berkeley, CA: Apress, 2024, pp. 45-89, https://doi.org/10.1007/979-8-8688-0315-4_2

[15] W. Zhang et al., "Application of machine learning, deep learning and optimization algorithms in geoengineering and geoscience: Comprehensive review and future challenge," Gondwana Research, vol. 109, pp. 1-17, 2022, https://doi.org/10.1016/j.gr.2022.03.015

[16] C. Chakraborty, Ed., Digital Health Transformation with Blockchain and Artificial Intelligence. CRC Press, 2022, https://doi.org/10.1201/9781003247128

[17] M. H. Alsharif, A. H. Kelechi, K. Yahya, and S. A. Chaudhry, "Machine learning algorithms for smart data analysis in internet of things environment: taxonomies and research trends," Symmetry, vol. 12, no. 1, p. 88, 2020, https://doi.org/10.3390/sym12010088

[18] S. Wadhwa and D. Gupta, "Blockchain Revolution: Using Distributed Ledger Technology to Transform Healthcare in WSN-IoT Environment," in Emerging Technologies and the Application of WSN and IoT, CRC Press, 2024, pp. 112-128. [Online]. Available: https://www.taylorfrancis.com

[19] M. E. E. Alahi et al., "Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: recent advancements and future trends," Sensors, vol. 23, no. 11, p. 5206, 2023, https://doi.org/10.3390/s23115206

[20] A. H. Sodhro, S. Pirbhulal, Z. Luo, and V. H. C. De Albuquerque, "Towards an optimal resource management for IoT based Green and sustainable smart cities," Journal of Cleaner Production, vol. 220, pp. 1167-1179, 2019, https://doi.org/10.1016/j.jclepro.2019.01.188

[21] S. Ahmed, "Enhancing Data Security and Transparency: The Role of Blockchain in Decentralized Systems," International Journal of Advanced Engineering, Management and Science, vol. 11, no. 1, p. 593258, 2025, https://doi.org/10.22161/ijaems

[22] S. S. Aravinth, "Unleashing the Power of Data and Security by Integrating Deep Learning and Blockchain in Smart City Infrastructure Development–A Future Perspective," in Deep Learning and Blockchain Technology for Smart and Sustainable Cities, Auerbach Publications, 2025, pp. 20-42, https://doi.org/10.1201/9781003476047

[23] P. R. Potdar and S. M. Parikh, "Internet of things (IoT) and artificial intelligence (AI) enabled framework for smart fleet management," OPSEARCH, pp. 1-33, 2025, https://doi.org/10.1007/s12597-025-00961-7

[24] R. Qaddoura, M. B. Younes, and A. Boukerche, "Towards optimal tuned machine learning techniques based vehicular traffic prediction for real roads scenarios," Ad Hoc Networks, vol. 161, p. 103508, 2024, https://doi.org/10.1016/j.adhoc.2024.103508

[25] S. Hira and S. Hira, "Smart energy management using vehicle-to-vehicle and vehicle-to-everything," in Artificial Intelligence-Empowered Modern Electric Vehicles in Smart Grid Systems, Elsevier, 2024, pp. 253-290, https://doi.org/10.1016/B978-0-443-23814-7.00010-9

[26] V. Astarita, V. P. Giofrè, G. Mirabelli, and V. Solina, "A review of blockchain-based systems in transportation," Information, vol. 11, no. 1, p. 21, 2019, https://doi.org/10.3390/info11010021

[27] D. Khan, L. T. Jung, and M. A. Hashmani, "Systematic literature review of challenges in blockchain scalability," Applied Sciences, vol. 11, no. 20, p. 9372, 2021, https://doi.org/10.3390/app11209372

[28] M. Merenda, C. Porcaro, and D. Iero, "Edge machine learning for ai-enabled iot devices: A review," Sensors, vol. 20, no. 9, p. 2533, 2020, https://doi.org/10.3390/s20092533

[29] O. Layode, H. N. N. Naiho, G. S. Adeleke, E. O. Udeh, and T. T. Labake, "Data privacy and security challenges in environmental research: Approaches to safeguarding sensitive information," International Journal of Applied Research in Social Sciences, vol. 6, no. 6, pp. 1193-1214, 2024, https://doi.org/10.51594/ijarss.v6i6.1210

[30] B. Alotaibi, "Utilizing blockchain to overcome cyber security concerns in the internet of things: A review," IEEE Sensors Journal, vol. 19, no. 23, pp. 10953-10971, 2019, https://doi.org/10.1109/JSEN.2019.2935035

[31] J. Li, "Governing High-Risk Technologies in a Fragmented World: Geopolitical Tensions, Regulatory Gaps, and Institutional Barriers to Global Cooperation," Fudan Journal of the Humanities and Social Sciences, pp. 1-25, 2025, https://doi.org/10.1007/s40647-025-00445-4

[32] A. Kulkarni and M. Bedekar, "Standardization in Cloud Computing: Unlocking the Potential of a Fragmented Industry," in International Conference on Advancements in Smart Computing and Information Security, Cham: Springer Nature Switzerland, Dec. 2023, pp. 3-12, https://doi.org/10.1007/978-3-031-59100-6_1

[33] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," International Journal of Production Research, vol. 57, no. 7, pp. 2117-2135, 2019, https://doi.org/10.1080/00207543.2018.1533261

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

[35] J. Lin et al., "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125-1142, 2017, https://doi.org/10.1109/JIOT.2017.2683200

[36] O. Riđić et al., "Implementation of blockchain technologies in smart cities, opportunities and challenges," in Blockchain Technologies for Sustainability, 2021, pp. 71-89, https://doi.org/10.1007/978-981-16-6301-7_4

[37] P. Sharma, R. Jindal, and M. D. Borah, "Blockchain technology for cloud storage: A systematic literature review," ACM Computing Surveys (CSUR), vol. 53, no. 4, pp. 1-32, 2020, https://doi.org/10.1145/3403954

[38] A. Rahman et al., "Impacts of blockchain in software-defined Internet of Things ecosystem with Network Function Virtualization for smart applications: Present perspectives and future directions," International Journal of Communication Systems, vol. 38, no. 1, p. e5429, 2025, https://doi.org/10.1002/dac.5429

[39] Z. Zhang, X. Song, L. Liu, J. Yin, Y. Wang, and D. Lan, "Recent advances in Blockchain and artificial intelligence integration: feasibility analysis, research issues, applications, challenges, and future work," Security and Communication Networks, vol. 2021, pp. 1-15, 2021, https://doi.org/10.1155/2021/9991535

[40] A. Nag et al., "Exploring the applications and security threats of Internet of Thing in the cloud computing paradigm: A comprehensive study on the cloud of things," Transactions on Emerging Telecommunications Technologies, vol. 35, no. 4, p. e4897, 2024, https://doi.org/10.1002/ett.4897

[41] E. Badidi, "Edge AI and Blockchain for smart sustainable cities: promise and potential," Sustainability, vol. 14, no. 13, p. 7609, 2022, https://doi.org/10.3390/su14137609

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

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

[44] P. Bothra, R. Karmakar, S. Bhattacharya, and S. De, "How can applications of blockchain and artificial intelligence improve performance of Internet of Things? – A survey," Computer Networks, vol. 224, no. May 2021, p. 109634, 2023, https://doi.org/10.1016/j. comnet.2023.109634

[45] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," Internet of Things (Netherlands), vol. 11, p. 100227, 2020, https://doi.org/10.1016/j.iot.2020.100227

[46] E. Fazel, M. Z. Nezhad, J. Rezazadeh, M. Moradi, and J. Ayoade, "IoT convergence with machine learning & blockchain: A review," Internet of Things (Netherlands), vol. 26, no. December 2023, p. 101187, 2024, https://doi.org/10.1016/j.iot.2024.101187

[47] T. Nguyen, H. Nguyen, and T. Nguyen Gia, "Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications," Journal of Network and Computer Applications, vol. 226, no. September 2023, p. 103884, 2024, https://doi.org/10.1016/j.jnca.2024.103884

[48] A. M. Shamsan Saleh, "Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review," Blockchain: Research and Applications, p. 100193, 2024, https://doi.org/10.1016/j. bcra.2024.100193

[49] P. Pandurangan et al., "Integrating cutting-edge technologies: AI, IoT, blockchain and nanotechnology for enhanced diagnosis and treatment of colorectal cancer - A review," Journal of Drug Delivery Science and Technology, vol. 91, no. August 2023, p. 105197, 2024, https://doi.org/10.1016/j.jddst.2023.105197

[50] Z. Kamal, M. Lachgar, and H. Hrimech,"Blockchain, IoT and AI in logistics and transportation: A systematic review," Transport Economics andManagement, vol. 2, no. July, pp. 275–285, 2024, https://doi.org/10.1016/j.team.2024.09.002

[51] V. V Prabhakar, C. S. Belarmin Xavier, and K. M. Abubeker, "A Review on Challenges and Solutions in the Implementation of Ai, IoT and Blockchain in Construction Industry," Materials Today: Proceedings, 2023, https://doi.org/10.1016/j.matpr.2023.03.535

[52] M. Gupta, M. Kumar, and R. Dhir, "Unleashing the prospective of blockchain-federated learning fusion for IoT security: A comprehensive review," Computer Science Review, vol. 54, no. June, p. 100685, 2024, https://doi.org/10.1016/j.cosrev.2024.100685