BIBLIOMETRIC ANALYSIS SUPPORTED REVIEW ON WEB 3.0 BASED DATA ANALYTICS FOR IIOT ENABLED SYSTEM

Nehaben Patel[1], Minal Shukla[2], Pooja Sapra[3], Amit Sata[4], Mrudul Jani[5], Pravin Vadhel[6]

[1,3]Department of Information Technology, PIET, Parul University, Vadodara, Gujarat, India
[2,5,6]Department of Applied Science and Humanities, PIET, Parul University, Vadodara, Gujarat, India
[4]Department of Mechanical Engineering, Marwadi University, Rajkot, Gujarat, India
[1]nehapatel57577@gmail.com

Keywords: Web 3.0, Data Analytics, Industrial Internet of Things, Blockchain, Bibliometric Analysis.

Abstract
Web 3.0 technology is currently attracting more attention regarding its critical application in the use of next-generation data analytics in the IIoT industry. Web 3.0 technology acts as a basis for the development of a distributed smart architecture in the IIoT industry. Various research studies have proved that the use of data analytics can generate a great improvement in the context of efficiency and decision-making in the IIoT industry. Scalability issues, interoperability issues, real-time data analytics, and issues of privacy are considered to be the challenges in the current data analytics systems in the IIoT industry. The review article will present a current understanding on the basis of the latest research studies on the application of Web 3.0 technology in the context of data analytics in the IIoT industry. Through systematic and bibliometric analysis, the paper identifies the research trends, thematic development, and research gaps in the available literature on data analytics in the Web 3.0-IIoT domain.

1 Introduction
Whereas it is true that web 2.0 development has made the Internet an interactive platform that now allows user interaction and content creation, such development has nonetheless continued to maintain centralized approaches in terms of the organization and control of data, along with all challenges related to data monopolization, data privacy, and data transparency, and need for trusted intermediaries[1][2], insofar as these features are increasingly out of place with respect to data-intensive multi-stakeholder IIoT networks[2]. Web 3.0 has its place in the new paradigm that is dependent on blockchain, Artificial intelligence, semantic web concepts, and storage networks with the aim of regaining control and trust between humans and computers [1],[3]. With its fundamentals dependent on trust, storage, and intelligent automation using blockchain concepts, web 3.0 provides the facility for trustworthy, self-sustained, and verifiable web activities [2]. Concomitant with these, the IIoT applications are characterized by very high volumes of varied data that require agile, secured, and real-time, analysis solutions. However, the existing IIoT adoption is still dominated by cloud-based solutions that are susceptible to security risks, real- time communication, and trust within the participants of the IIoT networks [4]. Therefore, the merging of Web 3.0 and the IIoT represents the imperative shift toward more trusted and smarter IIoT environments. In the beginning, the analytics process of the IIoT used architecture of cloud processing for the storage and processing of data with central servers. Though the biggening analytics process is successful, the process of processing latencies and privacy issues regarding the existing architecture were pointed out in [4]. Lately, there has been a lot emphasis on the decentralized analytics system and intelligence by means of Web 3.0 technologies. In addition to that, based on blockchain technologies for knowledge inference, geographically separated parties within the sector are able to participate collectively within intelligent fault diagnosis without exchanging data directly from the sources to protect data privacy [4]. Furthering the movement toward the decentralized analytics system is the federated analytics method that allows for local learning by means of the secure aggregation of data to reduce the cost of communication effectively while making sure that there is analytics accuracy at the same time [5]. In addition to that, by means of highly advanced methods for inferential leaning within the traffic reconstruction within tomographic networks, the feasibility of a decentralized analytics system within the web 3.0 environment has already proved to be achievable even under data incompleteness regardless of whether there are any errors within data itself [6]. The IIDM IIoT data analytics systems based on centralized architectures contain certain inherent drawback concerning the trust induced by single points of failure, increased susceptibility to cyberattacks, and ineffectiveness for supporting transparent auditing for data governance approaches [7]. Such architectural challenges will further destabilize trust levels for stakeholders taking part in any given transaction to ascertain collaborative efforts between organizations to some extent. Most of the above- depicted centralized architectures will fail to provide and appropriate incentive scheme for encouraging stakeholders to provide data contributions as well as computational contribution effectively. Real-world scenarios concerning a centralized recommendation service system for stakeholders and an e-waste disposal system will reveal that increased level of stakeholders taking active involvement will liaise with level of increased transparency and incentive alignment [8]. Another weakness is found to be linked to inefficient use of the resources

of dispersed computation, which has huge computation resources utilized at edge nodes and end user systems in terms of completely centralized control; some voluntary computing platforms have been designed to make use of unutilized and idle resources of the end user system nodes [9].

All of the aforementioned difficulties stress the need to move on to decentralized analytics system for web 3.0. As a correction for deficiencies in the data analytics process in a central authority, described in section 3.3, the approach in web 3.0 is a totally decentralized paradigm characterized by the interfacing of immutable ledger system and trust, he use of intelligent contract mechanisms and AI into itself. Blockchain ensures immutability in data storage, an element of decentralized consensus, and an audit trail, and hence removes the reliance on central authority, and also enhances the levels of trust in all stakeholders involved in the IIoT process [10]. Additionally, the complementing effect of AI and blockchain has also given rise to yet another concept of blockchain intelligence that enhances the efficiency and effectiveness of decisions made from analytics processes with AI's accountability, and AI's analytics efficiency with blockchain's properties of accountable, traceable, and trustworthy AI analytics processes [11]. Moreover, the role of decentralized applications in the context of web 3.0 explains how streams from analytics processes can be automated, auditable, and incentivized in a manner to foster stakeholder engagement and collaboration, and thus refers to [12]. By using concepts related to storage, interoperability, and identity, the Web 3.0 offers a scalability, security, and collaboration structure of analytics so as to counter the issues associated with centralized models, hence offering a robust foundation for sophisticated analysis in the Industrial Internet of things and hence ushering in developments in the next section. In spite of the fast-traced advancements in Web 3.0 technology, currently, the literature is still scattered across various domains, including blockchain, artificial intelligence, metaverse technology, and Industrial IoT networks. Currently, the scattered nature of the Web 3.0 literature identifies an enormous gap in the application of systematic approaches in knowledge synthesis. Systematic reviews of literature not only help in creating an empirical framework for the synthesis of scattered literature in all realms pertaining to web 3.0, but in the process, it also helps in identifying gaps in the literature, along with creating taxonomic constructs around them [13]. Alongside systematic reviews, a bibliometric analysis might help in unearthing other essential, quantifiable aspects related to publication, group-wise, as well as future development in web 3.0-related areas. Currently, diverse cross-industry needs for web 3.0 analytics, as explained in section 3.4, clearly elucidate that there is a need for a combination of systematic reviews of web 3.0- related literature along with the accompanying use of bibliometric analysis in helping in creating a macro view in the web 3.0 domain studied in this research work in entirely [14]. Through a compilation of information regarding the web 3.0-based analytics system and the correlated security issues and bibliographic trends, the contribution of this review presents a recent extension of existing work and sheds light upon some new aspects of web 3.0 that remain to be uncovered, especially for the Industrial Internet of Things (IIoT) paradigm [15]. Recent studies have demonstrated the effectiveness of integrating blockchain with IIoT systems to elevate trust, safe-guarding, and data-driven decision-making in industrial environments, particularly in manufacturing inspection and process optimization [16][17]. While these contributions validate the practical potential of decentralized architectures, the rapid and fragmented growth of related research highlights the need for a comprehensive bibliometric investigation. Accordingly, this study systematically analyses Web of Science–indexed literature to map the evolution, thematic structure, and research gaps of Web 3.0–based data analytics for IIoT-enabled systems.

2 Bibliometric

It is observed that popularity of Web 3.0 has been increased in last few years however an integration of Web 3.0 especially with IIoT application is yet to be fully explored. Detailed analysis of prior work-related research and development has been conducted using one of the most promising databases such as Web of Science®. Meaningful insights achieved from these databases are highlighted herewith. These databases were searched with keyword related to Web 3.0, and various types of documents were studied. Methodology adopted for this study of bibliometric analysis on Web 3.0 conducted using open-source platform, RStudio®, and is highlighted in table 1.

Table 1: Methodology adopted for bibliometric analysis

Database searched for documents published	Clarivate Web of Science™
Duration	2015-2025
Type	Articles, review articles, book chapter, early access, proceeding papers
Total number	3104
Language	English

It is observed little research and development work in this domain has been conducted in last few years, and seems to have very high potential for contribution. This analysis helped in deciding the direction for development of Web 3.0 framework especially for IIoT enabled system. Detailed discussion on Bibliometric analysis is presented here followed by methodology for development and demonstrative work supporting that methodology.

Overview

Table 2 represents the overview about bibliometric analysis carried out on documents published in both of databases.

Table 2: Overview of bibliometric analysis

Total documents	3104
Total number of sources (i.e., journal, conference, publishers) in which documents were published	1820
Average citation per document	~22.5
Total number of authors contributed	17302
International co-authorship (*in percentage*)	33.1

Distribution of overall documents published in Web of Science® is also shown in Figure1.

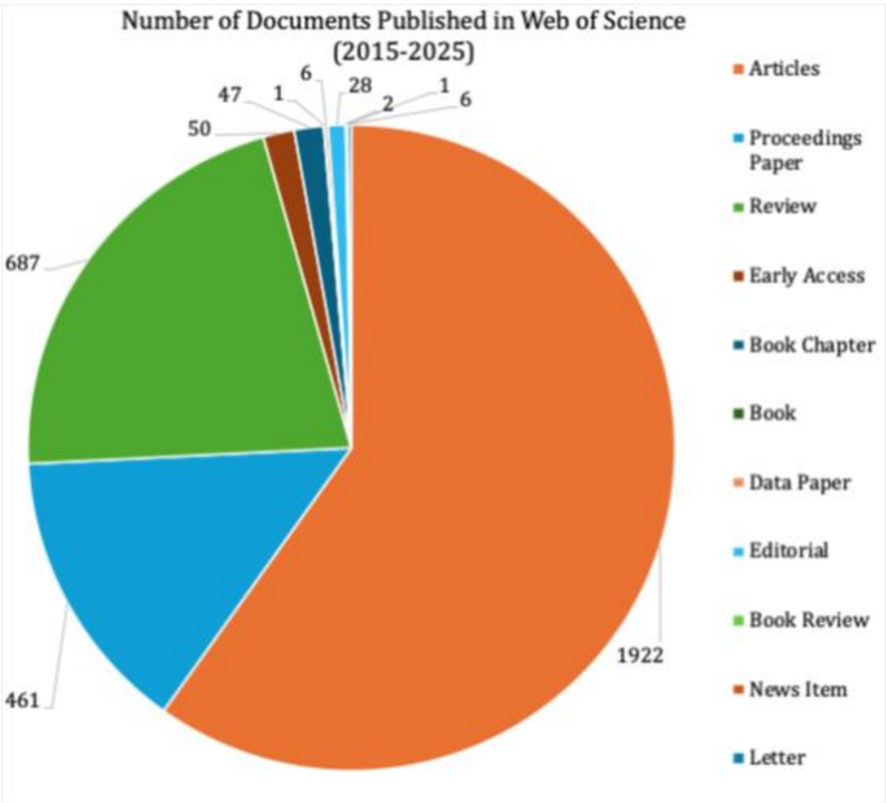

Figure 1: Type of documents published in Web of Science®

Year-wise publication is also checked (Figure 2), and it was observed that number of documents published in the domain of *Web 3.0* is increased since 2015 with average increasing rate of 16.75%, and nearly 3175 documents published in the year of 2024. However, slight reduction in number of publications is happened in the year of 2025 (till December 2025).

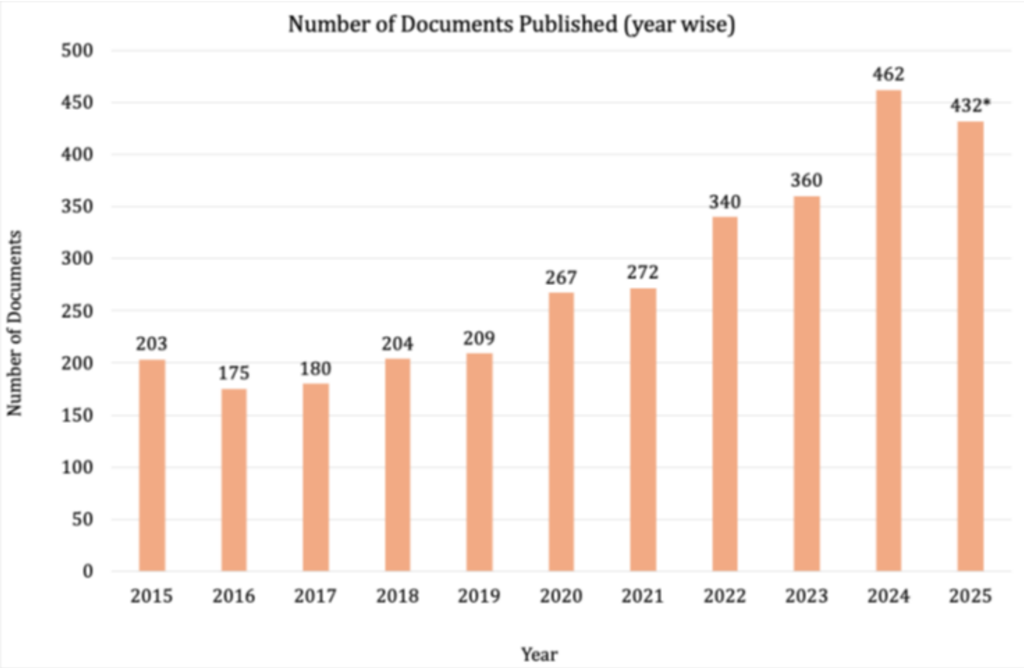

*Figure 2: Year wise publication of documents (*data is till December 2025)*

Major contributors including researcher's, their affiliation's, countries, sources, etc. are also found out using systematic bibliometric analysis, and is highlighted herewith.

Contributors and Collaboration

Authors conducted remarkable research in the domain of Web 3.0, and their publication, as well as h-index are represented in Figure 3. Dr. Zhang Y has highest number of documents published (i.e., 18) and *h-index* (=7) in this domain.

Also, most cited country and their average citations per document are shown in Figure 4. It is observed that USA has maximum number of citations followed by China and Canada. However, average citations per article is highest for Georgia (~210) followed by Norway (~150). Average citations per article is for India is relatively low, and in the range of 7.7.

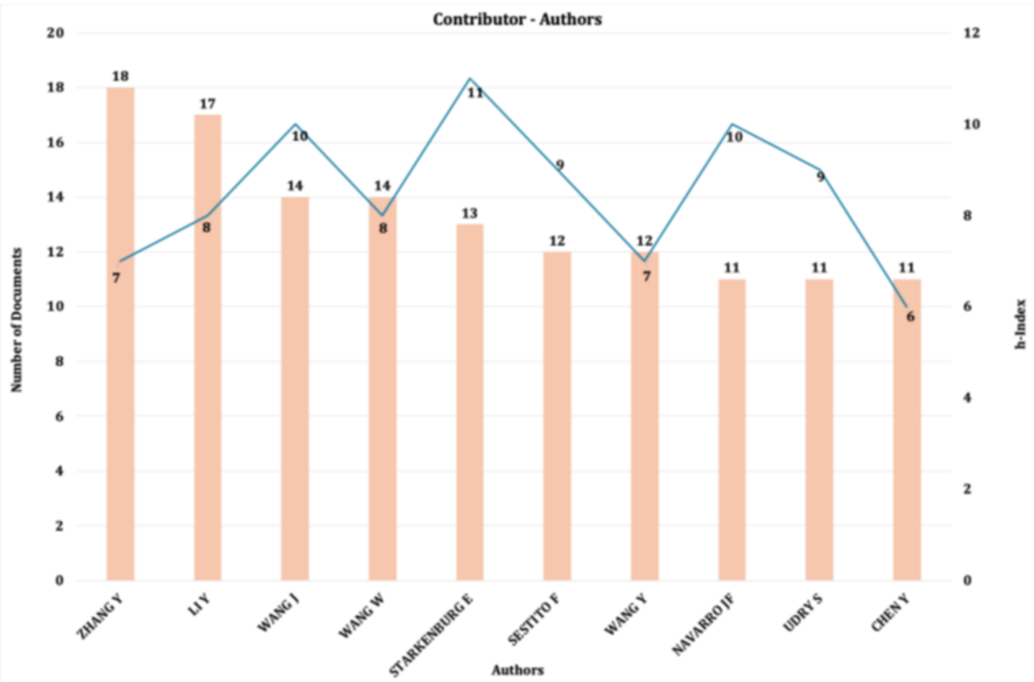

Figure 3: Top 10 Authors, and Their h index

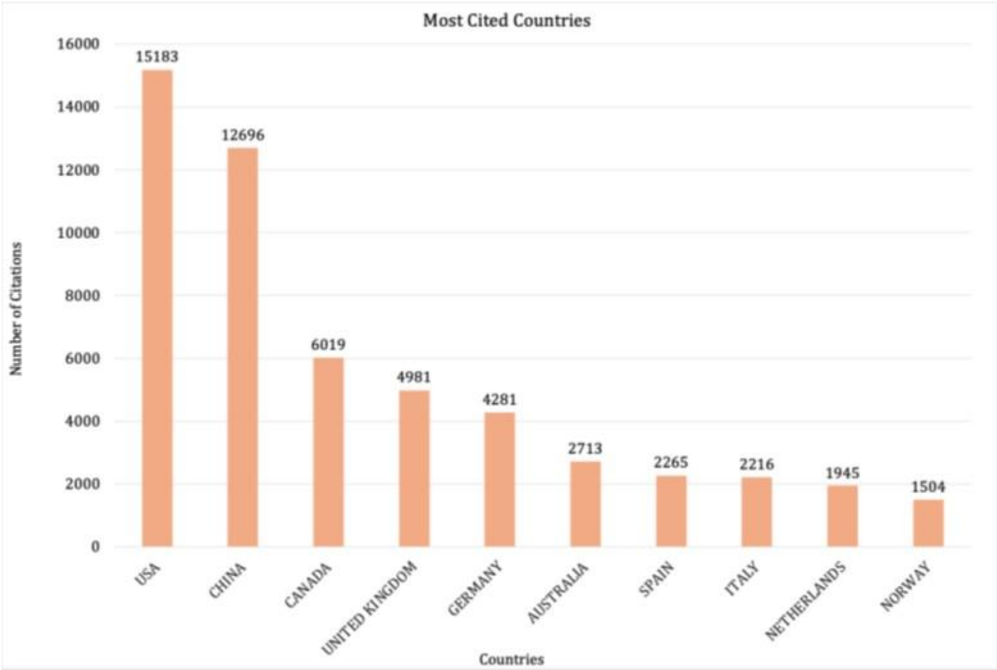

Figure 4: Most cited Countries

Specific three-field plot is generated highlighting authors, affliated institutes and countries to highlight contribution, and is illustrated in Figure5. It is observed that Dr Udry S from Chinese Academy of Sciences – China have remarkably contributed in this domain.

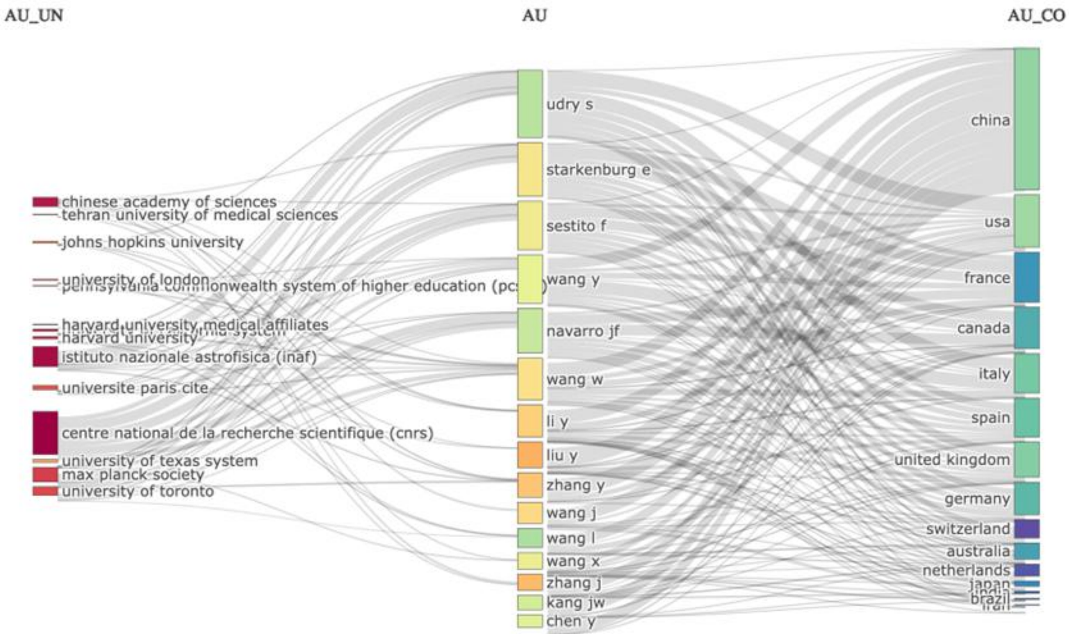

Figure 5: Three field plot highlighting institutes, authors and countries working in this domain

Collaborative research plays very important role especially in this domain. It was observed that 33.1% of documents has international co-authorship, and overview of collaboration between various countries is shown in Figure 6. USA has developed strong collaboration with UK for 131 documents and with China for 98 documents. USA has published 97 documents with Germany; 85 documents with Canada; 82 with UK; with France 74 documents; and 73 documents with Italy. India has published 26 documents with USA; and 15 with UK. However, collaboration of India with China, Canada, France, Japan, Germany, etc. can be strengthen in this domain.

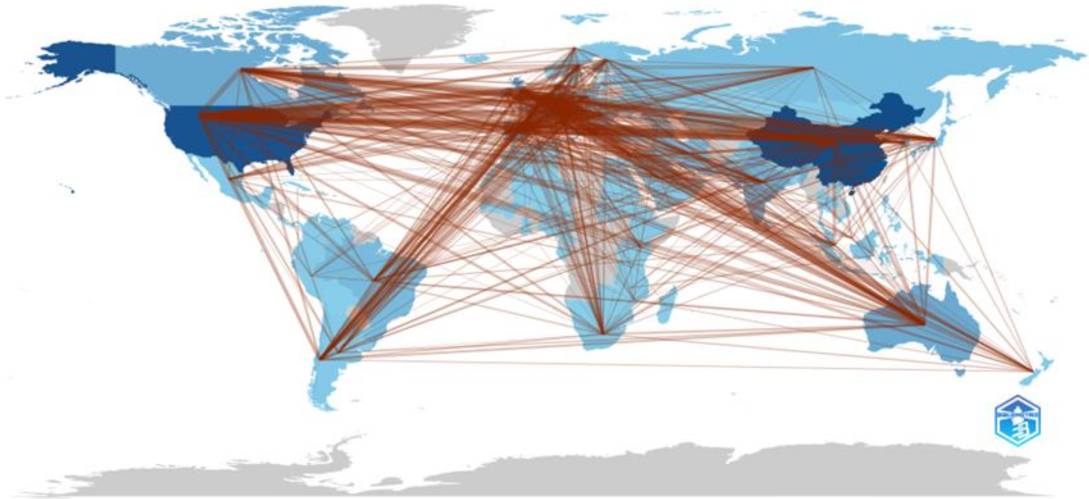

Figure 6: Collaboration between various countries for research in the domain of Image Processing for Manufacturing

Various keywords used other than in these documents were also studied, and observed that keyword related to IIoT with Web 3.0 is not fully explored. Detailed technical literature highlighting application of Web 3.0 for IIoT application is summarized next.

3 Prior Work

The IIoT platforms established by Web 3.0 result in a revolution in identify and access management with a paradigm shift from a centralized model to a trust-based, decentralized system. The conventional identify management service uses a centralized system, creating Single Points of failure, which makes trusts between different entities a necessity in various industries affecting identity management service scalability and security [18]. The trustworthy decentralized identity system using blockchain provides the IIoT participant with the capability for autonomous verification and interaction without the need for any kind of central entity or authority. Data integrity and/or any kind of tampering is ensured through cryptographic proofs and Merkle hash-tree data storage methods [18]. Any kind of access to the identity information is also improved through the application of the authenticated data structures that support secure queries for both real-time and historic identity information for the dementalized identity systems [19]. Decentralized access control system utilizes blockchain and smart-contracts to implement the rules of access within a secure, server-free environment. These ensure immutable auditing trails, increase resilience to impersonation attacks, and support detailed access control for IIoT devices [20]. Furthermore, digital wallet frameworks for the universal level bridge the limitations of compatibility and support for decentralized settings, allowing for a unified concept of identity, payment services, and provable documents under user control [21]. Web 3.0-based data analytics techniques in the context of IIoT make use of the integration of blockchain technology, artificial intelligence, and storage solutions that work towards meeting the core requirements related to data security, privacy, and intelligence. Blockchain-based deep leaning approaches show the integration of secure data storage techniques with smart contacts, which can be applied in the healthcare domain due to security concerns related to data integrity in healthcare-related service [22]. Models of analytics of the digital twin include the capabilities of the IIoT through the use of virtual replicas for physical systems. In addition, the application of web 3.0 infrastructural systems provides assurance of having the benefits of system synchronization and web 3.0 infrastructural analytics, which could enhance the accuracy of system and predictive analysis [23]. Also, through the application of the task of loading of the reinforcement learning exchange, the optimal support is achieved for the systems with the digital twin [24]. In resource-constrained IIoT networks, effective analytics techniques should be applied to guarantee that the performance of systems works within expectations. Test-time adaptation techniques can aid models to adapt at test time without training requirements [25]. Blockchain is used as a basis for trust in decentralized data analysis in IIoT because it allows for immutable data storage, audit trails, and decentralized consensus without involving trusted third parties. Although both characteristics make it possible to ensure secure and stable data analysis in a web 3.0 setting, vulnerabilities in smart contracts have emerged as a serious- concern in regard to data analysis security. The challenge in ensuring data analysis security has been addresses in research involving sophisticated vulnerability analysis frameworks utilizing both graph-based models and attention-driven deep learning approaches, outperforming conventional rule-driven tools in regard to detection precision and reduced falsely detected vulnerabilities [26]. Consensus algorithm plays major roles in determining scalability and decentralization in blockchain-based IIoT networks. Improved versions of delegated consensus algorithm with quadratic voting systems mitigate problems related to stake centralization and a low level of stake holder participation by readjusting stake holder voting rights and ensuring fairer stake holder equity [27]. Additionally, blockchain consortia are applied in the process of data integrity auditing, which relies on consortium blockchain networks instead of third-party auditors for data integrity with optimized Merkle hash tree formulation and non-node point sampling techniques to ensure privacy- preserving operations for dynamic data for data integrity checks

[28]. Because of inherent latency, scalability, and privacy limitations, purely cloud-centric computing approaches are inadequate for web 3.0 enabled IIoT systems. Such limitations are overcome by the mobile edge computing architectures designed for web 3.0, which integrate blockchain and artificial intelligence to offer secure, low- latency services over 5G and emerging 6G networks. It leverages intelligent resource allocation, secure edge level processing, and adaptive quality-of-service mechanisms for efficient handling of diverse Industrial workloads [29]. Beyond MEC, decentralized edge computing frameworks enhance system resilience through enabling peer-to-peer collaboration between distributed nodes, while unified blockchain-semantic frameworks improve efficiency and scalability through reducing on-chain data redundancy by promoting verified off-chain semantic data interactions [30]. Further, blockchain-based crowdsourcing computational tasks, which allows trustless execution, and fair incentive distribution enables the utilization of idle resources effectively across IIoT environments [31]. Recent studies have also explored the use of generative AI in Web 3.0 settings, particularly in the optimization of analytics and content control [32]. Semantic data trading with the use of blockchain-enabled architectures improves trust and data quality in decentralized market [33], while data annotation platforms in Web 3.0 can also promote fair data sharing with reward schemes for data contributors [34]. While machine learning-based task scheduling and volunteer computing optimize resource utilization, they introduce control, trust, interoperability, and privacy problems, and forensic-driven resource allocation improves accountability but risks introducing complexity and degrading real-time performance. Web 3.0 facilitates decentralized data analysis using blockchain-based processing, which helps in reliable data analysis without the need for centralized control in the IIoT context [35]. Blockchain consensus algorithms, such as incentive-based and secure PBFT, improve the reliability and integrity of data but are challenged by scalability issues when dealing with industrial loads [36], [37]. Secure data sharing in Web 3.0-enabled IIoT is achieved through encryption-based storage [38], decentralized identity and account management [39], cross-platform authentication [40], and smart contract- based access control [41], whereas privacy-preserving data analysis using homomorphic encryption [42] and federated learning [43] keeps on posing efficiency and trust-related challenges in real-time data analysis.

4 Methodology

In this study, the systematic literature review method is employed to investigate the current literature on data analytics in the context of Web 3.0 and the Industrial Internet of Things (IIoT). Since the topic of interest is interdisciplinary, involving blockchain, artificial intelligence, and data analytics, a structured multi-keyword search method was employed. The keywords used involved the core technologies of Web 3.0 and the application domains associated with the IIoT. To ensure the relevance and quality of the literature selected, inclusion and exclusion criteria were set prior to the literature screening process.

Inclusion criteria

The review considered peer-reviewed studies that:

1. Deal with Web 3.0 technologies such as blockchain, decentralized identity, intelligent contracts, semantic web, and decentralized artificial intelligence.
2. Describe data analytics, learning, or intelligent decision-making models for IIoT or cyber-physical systems.
3. Discuss conceptual framework, system architectures, algorithms, simulations, or empirical studies related to decentralized data analytics.

Exclusion criteria

The review excluded studies that:

1. Primarily deal with Web 2.0 or centralized systems that are not relevant to decentralization.
2. Lack technical or methodological rigor.
3. Are non-peer-reviewed sources such as editorials, tutorials, or opinion pieces.
4. Are not directly related to data analytics, intelligent processing, or trust mechanisms for IIoT or cyber-physical systems.

By using these criteria, the review was able to include high- quality literature that is relevant to the topic, while also reducing redundancy and irrelevant information.

The Architecture of Web 3.0-enabled data analytics systems is a significant aspect of system scalability, trust management, system latency, and resource utilization, especially in the context of IIoT networks. From the existing literature, it has been recognized that the architectures of Web 3.0-enabled data analytics systems can be classified into centralized-enhanced architectures, hybrid architectures, and fully decentralized architectures. Hybrid architectures are an intermediate approach that attempt to strike a balance between system efficiency and trust by leveraging cloud resources along with edge computing or blockchain support. In hybrid architecture, mobile edge computing, intelligence resource management, and trajectory planning can enable real-time data analysis with reduced reliance on centralized coordination. Conversely, the fundamental idea of Web 3.0 is implemented architecture, in which there is no central control over the entire system. In fully decentralized architecture, computation, storage, and administrative tasks are distributed across interlinked nodes that operate on a peer-to-peer basis. Blockchain and smart contracts are commonly used to build trust, automate processes, and implement incentive schemes without relying on centralized systems.

Fully decentralized architectures embody the essential paradigm of Web 3.0, which emphasizes novel efficiency and complexity issues related to data analytics in IIoT settings. In addition to the architectural aspect, data analytics systems based on Web 3.0 also utilize various techniques of analysis to support decentralized intelligence, privacy, and scalability. Various techniques have been proposed to improve the traditional machine learning model to function in a trustless and decentralized environment. Among these, split learning and cooperative learning have been identified as important privacy-preserving analytics methods for Web 3.0 applications. In these methods, multiple parties can work together to train machine learning models without accessing the original data, but by accessing the secure intermediate representations. In particular, the application of privacy- preserving vertical co-operative leaning makes it extremely suitable for application within an industrial environment that has stringent privacy considerations. This is particularly the case with advanced analytics, such as the application of generative AI models for 3D volumetric and latent diffusion data, where high-quality analytics can be accomplished through the application of distributed computational and graphical resources within Web 3.0-enabled IIoT systems. The application of these analytics methodologies is a paradigm shift from the conventional standardized processing models to the more IIoT-centric Web 3.0 models. Data management and trust building in Web 3.0 analytics platforms are inherently enabled by blockchain technology. The essential features of blockchain technology, such as immutability, distributed consensus, and transparency in auditing, provide a foundation for trust in decentralized collaborative platforms. In addition, blockchain-based frameworks for semantic analysis enhance the trustworthiness of data trading and sharing by combining semantic verification with immutability in transaction data, which ensures that the shared data in the decentralized marketplace is trustworthy and semantically consistent. The proposed frameworks involve the semantic of data into smart contracts, hence decreasing information asymmetry and facilitating trustworthy data trading and sharing between data providers and data seekers. Decentralized trade and annotation platforms play a critical role in data management, as they guarantee that data pricing, ownership, and access rights are followed in blockchain-based analytics and processing environments. Web 3.0-based data trading platforms facilitate the use of efficient data pricing models that promote the sharing of quality data while ensuring fair and transparent compensation for data partners. This trust model can be used in the IIoT data exchange environment, where trust and accountability are of utmost importance. Trust models constructed using blockchain technology offer a reliable platform for building decentralized analytics systems using immutability, smart contracts, and reward. Artificial intelligence is also a major facilitator of intelligent decision- making in Web 3.0 analytics systems. Together with decentralized systems, artificial intelligence makes it possible to have self-sustaining, adaptive, and context-aware analytics systems in decentralized settings. Natural language processing and learning analytics on blockchain-based Web 3.0 platforms have demonstrated the viability of decentralized AI in dealing with unstructured industrial and social data. Knowledge inference models help in intelligent fault detection and predictive analysis in IIoT, while generative AI helps in analytics of Web 3.0 through decentralized content generation, transformation, and optimization. Collaborative analytics help in fault and anomaly detection for various industrial entities without requiring access to their original sensor data, thus maintaining data ownership and privacy. The aforementioned techniques showcase the complementarity of AI-based analytics and the decentralized architecture of Web 3.0, thus moving ahead from rule-based industrial systems to autonomous, self-learning, and adaptive IIoT analytics. The key requirements in this regard are integrity, robustness, and secure decentralized data processing and exchange. Although blockchain technology provides immutability, transparency, and security, scalability issues in blockchain technology exist with regard to dynamic data auditing and privacy. Integrity auditing with blockchain technology is less dependent on third-party entities but faces scalability issues at the industrial scale. Consensus algorithms like PBFT provide robustness but are communication expensive, and incentive-driven algorithms are efficient in participation but are complex to design. More recent secure versions of PBFT have demonstrated stronger robustness and throughput performance; however, their applicability within highly resource-constrained IIoT settings remains an open issue. Secure storage systems enable data integrity within Web 3.0- enabled IIoT networks by enforcing strong cryptographic access control. Although the the expressive power of CP- ABE access control mechanisms is of a high level, it is still computationally expensive and inefficient in terms of key management and policy updates, hence not so ideal for resource-constrained IIoT devices, thus the need for more scalable solutions. Access control and authentication are very important in handling the issue of unauthorized access and insider threats in the Web 3.0 decentralized network. Thrustless systems are not compatible with centralized authentication systems; hence, the need for verifiable and tamper-proof identity and access control system. Blockchain- enabled decentralized portal architectures enable anonymous yet accountable authentication using cryptographic proofs and credentials, improving privacy and impersonation resistance. Nonetheless, challenges related to credential revocation, scalability, and usability persist in large-scale IIoT deployments. Cross-platform authentication using blockchain technology supports privacy-preserving and traceable identity verification, but the trade-off between anonymity and traceability in an industrial setting still poses a challenge. Access control systems using smart contracts enhance automation, auditability, and accountability, but contract-related attacks, insider threats, and privilege escalation attacks still exist, and formal verification for secure verification is a major challenge in Web 3.0-based IIoT analytics.

Although there is greater transparency, there are also privacy concerns that arise with decentralization because of the metadata that is revealed through the blockchain. Fully homomorphic encryption enables computations to be carried out on encrypted data, but this is very costly in terms of computational complexity. Federated learning is more privacy-preserving because less raw data is shared, but it is still susceptible to poisoning attacks, inference attacks, and Byzantine attacks, although there are trust-enhanced versions that are more robust but also more costly. Scalability and performance problems are also a hindrance to the use of Web 3.0 in IIoT analytics because the latency and throughput of blockchain networks grow with the size of the network. Graph attention-based dissemination and age-of-information optimization improve throughput and latency, respectively, but introduce complexity and the risk of incentive misalignment. These problems are further exacerbated by the resource constraints of IIoT and the expense of blockchain, cryptography, and distributed learning.

5 Research Gap

The current Web 3.0 analytics models focus on distributed structure and reliability but ignore the performance growth, data confidentiality, as well as low-latency demands of IIoT environments. The blockchain validation mechanisms improve protection but are still restricted due to delay problems and expansion limitations when dealing with large- scale industrial tasks. Privacy-enhancing approaches are linked to heavy computational burden and reliability expenses, making them unsuitable for limited-capacity IIoT applications.

Smart contract-enabled access management and distributed identity mechanisms improve automated operations and seamless integration but are still affected by validation, malicious insiders, data confidentiality, and legal constraints. As such, the absence of a holistic, complete Web 3.0 data analysis system for IIoT is a critical open issue.

6 Future Work

Future studies can include implementing a extensive complete Web 3.0 analytics solution that jointly addresses the performance growth, privacy assurance, and real-time low- latency demands of IIoT environments. Additional studies are required to examine the creation of robust and scalable agreement mechanisms that are more suitable for the low- resource industrial environment. Enhancing confidentiality- focused analytics with reduced processing overhead, as well as mathematically proven smart contracts for protected access management, is still a key challenge. Finally, future research should also explore dynamic trust-based learning and access validation methods that can effectively manage data protection, tracking capability, and legal obligations in the industrial environment.

7 Conclusion

This paper provided an extensive structured and bibliometric analysis of Web 3.0 driven analytics for IoT an IIoT- supported systems, focusing on the inherent drawbacks of traditional Web 2.0 framework. It is clear from the analysis that the implementation of blockchain technology, artificial intelligence, decentralized systems, and edge intelligence makes collaborative analytics possible in an intelligent and reliable manner. The paradigms shift in the decentralized and federated analytics architecture is well identified, which offers immense advantages in terms of data ownership, privacy conservation, system resilience, and real-time decision support. In addition, a taxonomy is also provided to systematically classify the existing research contribution s based on architectural paradigms, analytics methods, blockchain-based decentralization and trust models, and AI- based intelligence. Although significant process has been achieved, still some key challenges persist, particularly in terms of scalability, cross-platform interoperability, security constraints, and the lack of large-scale industrial validation. To address challenges, experimental validation in real-world IIoT applications and the development of interoperable, scalable, and privacy-preserving analytics platforms is required. The results and recommendations summarized in this research contribution constitute a knowledge base and serve as a foundation for future research and development of Web 3.0-based data analytics in industrial applications.

8 References

[1] G. Kumar, P. Rajakumar, Y. Dutt, R. Kumar, and Indervati, “The design and development of Web 3.0: The Internet’s future architecture,” *Proc. 1st Int. Conf. Advances in Computing, Communication and Networking (ICAC2N)*, IEEE, pp. 244–248, 2024.

[2] K. Vayadande et al., “Exploring the frontiers of blockchain and Web technologies for a dynamic digital future,” *Proc. 2nd Int. Conf. Inventive Computing and Informatics (ICICI)*, IEEE, Art. no. 00124, 2024.

[3] K. Vayadande et al., “A comprehensive review on navigating the Web 3.0 landscape,” *Proc. 2nd Int. Conf. Inventive Computing and Informatics (ICICI)*, IEEE, Art. no. 00080, 2024.

[4] Y. Chi, H. Duan, Z. J. Wang, W. Cai, and V. C. M. Leung, “Knowledge inference over Web 3.0 for intelligent fault diagnosis in Industrial Internet of Things,” *IEEE Trans. Network Science and Engineering*, vol. 11, no. 5, pp. 3955– 3967, Sep./Oct. 2024, doi: 10.1109/TNSE.2024.3389412.

[5] Z. Wang et al., “Federated analytics-empowered frequent pattern mining for decentralized Web 3.0 applications,” *Proc. IEEE INFOCOM*, Vancouver, BC, Canada, pp. 1–10, 2024, doi: 10.1109/INFOCOM53939.2024.10621231.

[6] C. Wang et al., “OD traffic maps recovery for Web 3.0 by network tomography in Hankel tensor space,” *IEEE Trans. Network Science and Engineering*, vol. 12, no. 3, pp. 1981– 1992, May/Jun. 2025, doi: 10.1109/TNSE.2025.3448129.

[7] Y. Huang et al., “Blockchain-enabled personalized travel recommendations with semantic search and transparent data,” *Proc. IEEE ICCCN*, pp. 1–10, 2025.

[8] R. M. Samuel et al., “Web 3.0 and NFTs enabled eWaste management system for smart city,” *Proc. IEEE WiSPNET*, pp. 1–6, 2023, doi: 10.1109/WiSPNET58512.2023.10143892.

[9] A. Antelmi et al., “A volunteer computing architecture for computational workflows on decentralized Web,” *IEEE Access*, vol. 10, pp. 98993–99010, 2022, doi: 10.1109/ACCESS.2022.3208476.

[10] J. Li et al., “Blockchain intelligence: Intelligent blockchains for Web 3.0 and beyond,” *IEEE Trans. Syst., Man, Cybern.: Syst.*, vol. 54, no. 11, pp. 6633–6642, Nov. 2024, doi: 10.1109/TSMC.2024.3369124.

[11] W. Li, “Smart blockchain and AI empowered Web 3.0,” *Proc. IEEE ICEIEC*, pp. 1–7, 2024.

[12] A. Sahu et al., “Web 3.0 decentralized application using blockchain technology,” *Proc. IEEE I3CS*, pp. 1–6, 2023.

[13] M. Hemashree et al., “Tagging of multimedia contents on the Web 3.0 using semantic artificial intelligence: A systematic literature review,” *IEEE Access*, vol. 13, pp. 142900–142921, 2025, doi: 10.1109/ACCESS.2025.3478121.

[14] A. Ghosh et al., “A survey on decentralized metaverse using blockchain and Web 3.0 technologies,” *IEEE Access*, vol. 12, pp. 146915–146948, 2024, doi: 10.1109/ACCESS.2024.3409815.

[15] D. Camacho Leal et al., “Metastudents in the metaverse: Navigating the shift to Web 3.0 education,” *Proc. IEEE EDUCON*, Monterrey, Mexico, pp. 1–8, 2024, doi: 10.1109/EDUCON58619.2024.10579361.

[16] N. Yousef, A. Sata, M. Shukla, S. Jarboui, and D. Mobarsa, “Blockchain-integrated IoT device for advanced inspection of casting defects,” *Scientific Reports*, vol. 15, Art. no. 5300, 2025, doi: 10.1038/s41598-025-86777-3.

[17] D. Mobarsa, A. Sata, M. Shukla, and P. K. Dutta, “Blending blockchain with manufacturing for developing smart and secure process: A review, framework and implementation,” in *Proc. 9th Int. Congr. on 3D Printing Technologies and Digital Industry*, Cluj-Napoca, Romania, Sept. 18–19, 2025.

[18] C. Qiu et al., “Blockchain-based verifiable decentralized identities for cyber-physical Web 3.0,” *Proc. IEEE ICaMaL*, 2024.

[19] J. Sheng et al., “Authenticated decentralized identifier retrieval for blockchain-based Web 3.0,” *Proc. IEEE GLOBECOM*, 2024.

[20] E. Aruna et al., “A Web 3.0 integrated blockchain- enabled access system,” *IEEE Trans. Consumer Electronics*, vol. 71, no. 1, pp. 1201–1210, Feb. 2025, doi: 10.1109/TCE.2024.3449921.

[21] G.-H. Kim, “A study on universal digital wallet for Web 3.0,” *Proc. IEEE ICUFN*, 2024.

[22] S. Mohamed et al., “An efficient blockchain and deep learning-based framework for secure healthcare data management,” *Proc. IEEE ICCCT*, 2025.

[23] K. A. Awan et al., “MediTwin: A Web 3.0-integrated digital twin,” *IEEE Trans. Consumer Electronics*, vol. 70, no. 3, pp.5654–5661, Aug.2024, doi: 10.1109/TCE.2024.3397812.

[24] Q. Wang et al., “Low-latency communications for digital twin empowered Web 3.0,” *IEEE Network*, vol. 37, no. 6, pp. 26–33, Nov./Dec. 2023, doi: 10.1109/MNET.2023.3321912.

[25] D. Seo et al., “Lightweight test-time adaptation for robust out-of-distribution face recognition,” *J. Web Engineering*, vol. 24, no. 6, pp. 871–910, 2025.

[26] Y. Cao et al., “SCcheck: Smart contract vulnerability detection for Web 3.0,” *IEEE Trans. Network Science and Engineering*, vol. 11, no. 5, pp. 4007–4019, Sep./Oct. 2024, doi: 10.1109/TNSE.2024.3391127.

[27] T. Lei et al., “Q-DPoS: Improved DPoS consensus for Web 3.0,” *Proc. IEEE GBC*, pp. 1–8, 2025.

[28] C. Wang et al., “Blockchain-based dynamic cloud data integrity auditing,” *IEEE Trans. Network Science and Engineering*, vol. 11, no. 5, pp. 3931–3942, Sep./Oct. 2024, doi: 10.1109/TNSE.2024.3387714.

[29] R. David et al., “Architecting mobile edge computing for Web 3.0 services,” *Proc. IEEE IHCSP*, 2024.

[30] Y. Lin et al., “A unified blockchain-semantic framework for Web 3.0,” *IEEE Wireless Communications*, vol. 31, no. 2, pp. 126–133, Apr. 2024, doi: 10.1109/MWC.2024.3364471.

[31] B. Ghimire et al., “Crowdsourcing computation in Web 3.0,” *Proc. IEEE MetaCom*, pp. 421–429, 2025.

[32] H. Park et al., “Mesh enhancement using generative AI for Web 3.0,” *IEEE Access*, vol. 13, 2025, doi: 10.1109/ACCESS.2025.3489210.

[33] J. Tan et al., “Blockchain-enforced semantic data trading,” *Proc. IEEE ICBCTIS*, pp. 1–6, 2024.

[34] S. Yang et al., “Web 3.0-based data annotation trading platform,” *IEEE Trans. Network Science and Engineering*, vol. 11, no. 5, pp. 4032–4044, 2024, doi: 10.1109/TNSE.2024.3392238.

[35] S. Saxena et al., “Hate discourse detection using Web 3.0,” *Proc. IEEE IC3I*, pp. 142–146, 2023.

[36] Z. Gao et al., “CD-PBFT: Incentive-based blockchain consensus,” *Proc. IEEE MetaCom*, pp. 441–448, 2023.

[37] Y. Zhao et al., “KR-PBFT: Secure consensus for Web 3.0,” *Proc. IEEE ISPA*, pp. 1994–1999, 2024.

[38] B. Gong et al., “Secure data storage using ABE in Web 3.0,” *IEEE Network*, vol. 37, no. 6, pp. 49–56, Nov./Dec. 2023, doi: 10.1109/MNET.2023.3321919.

[39] T. Wang et al., “Account service network for Web 3.0,” *IEEE Network*, vol. 37, no. 6, pp. 108–115, 2023, doi: 10.1109/MNET.2023.3321926.

[40] G. Thakur et al., “Cross-platform authenticationfor metaverse in Web 3.0,” *IEEE Open J. Commun. Soc.*, vol. 5, pp. 1–19, 2024, doi: 10.1109/OJCOMS.2024.3369012.

[41] G. Thakur et al., “Smart contract-based authentication for Web 3.0 metaverse,” *IEEE Trans. Consumer Electronics*, early access, 2025, doi: 10.1109/TCE.2025.3481129.

[42] B. S. Goryachkin and E. D. Vdovkina, “Data security in Web 3.0 using homomorphic encryption,” *Proc. IEEE REEPE*, pp. 1–6, 2024.

[43] Z. Yuan et al., “Trustworthy federated learning in Web 3.0,” *IEEE Trans. Network Science and Engineering*, vol. 11, no. 5, pp. 3969–3982, 2024, doi: 10.1109/TNSE.2024.3389981.