Vol. 7, No. 4, December 2025

ISI Journal of Information Systems and Informatics

Published By Asosiasi Doktor Sistem Informasi Indonesia

Trends of Machine Learning, Cybersecurity and Big Data Analytics in Industry 4.0

Md. Mostakim Sarker[1], Md. Jahid Hasan Jony[2], Md Wali Ullah[3], Jannat Begum[4], Nusaibah Naushin[5*]

[1]Department of Management Information Systems, University of Dhaka, Dhaka, Dhaka-1000, Bangladesh

[2,4,5*]Department of Management Information Systems, Begum Rokeya University, Rangpur, Bangladesh

[3]MBA, Information Technology, Westcliff University, Irvine, United States of America

Email: mdmostakim-15-2019913041@mis.du.ac.bd[1], jahidhasanjony515@gmail.com[2], m.ullah.117@westcliff.edu[3], jannat.12222024@student.brur.ac.bd[4], nusaibah.12022025@student.brur.ac.bd[5*]

Received: October 5, 2025

Revised: November 7, 2025

Accepted: Nov 12, 2025

Published: Dec 9, 2025

Corresponding Author:

Author Name*:

Nusaibah Naushin

Email*:

nusaibah.12022025@student.brur.ac.bd[5*]

DOI:

10.63158/journalisi.v7i4.1321

Abstract. This research explores the integration of Machine Learning (ML), Cybersecurity, and Big Data Analytics (BDA) in advancing intelligent, secure, and sustainable industrial ecosystems within Industry 4.0. It assesses global research productivity, collaboration patterns, and the connection between intelligent automation, data-driven innovation, and cyber resilience. A PRISMA-based bibliometric review of 1,386 relevant publications from the Scopus database (2020-2025) was conducted, using Biblioshiny visualization tools to map key authors, institutions, countries, and emerging research clusters. Findings show a 7.09% annual growth in publications, reflecting a growing global focus on ML, BDA, and cybersecurity within Industry 4.0 ecosystems. The United States, China, and India were identified as major contributors, with strong cross-continental collaborations fostering innovation. Key research topics include deep learning, digital twins, and the Internet of Things (IoT), while emerging areas such as explainable AI, federated analytics, and edge computing are gaining attention. By mapping global research dynamics and identifying key contributors, this study highlights critical research gaps and offers practical insights for advancing interdisciplinary innovation, aimed at creating secure, intelligent, and sustainable industrial ecosystems in Industry 4.0.

Keywords: Machine learning; Cyber Security; Artificial Intelligence; Big data; Industry 4.0; Learning systems; Biblioshiny

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

1. INTRODUCTION

The emergence of the Fourth Industrial Revolution (Industry 4.0), driven by the Internet of Things (IoT) and Cyber Physical Systems (CPS), has fundamentally changed the global industrial and manufacturing paradigm [1]. Networked intelligent factories are being created by this revolution, generating new amounts of high velocity data. Utilizing this data to create better and more intelligent products requires sophisticated analysis tools [2]. In particular, machine learning (ML) enables the development of autonomous and predictive decision-making functions that are crucial for efficiency and flexibility, while big data analytics (BDA) provides the knowledge to manage these enormous streams.

Data-driven intelligence and automation are made possible by machine learning (ML), which supports Industry 4.0. ML algorithms examine intricate data patterns, increasing decision-making precision and system flexibility in logistics, manufacturing, and quality control [3]. Example of Industry 4.0 like automation, cyber-physical systems, and digital transformation, is the fourth industrial revolution. It combines smart technologies to build data-driven, connected, and flexible production environments that boost creativity and operational effectiveness [4-8].

The issue statement and research problem, when measured by the conciseness of their definition, are literally created to fill the existent gap in knowledge regarding the integrated role of Machine Learning (ML), Big Data Analytics (BDA), and Cybersecurity in the Industry 4.0 [4]. The issue is that the existing literature is fragmented, including the studies that tend to study these domains separately without delving into the prospect of their synergy in achieving intelligent, secure, and sustainable industrial systems. The problem of this study is clearly defined as focusing on the fact that there is no single theoretical and empirical framework that explains how these technologies can be combined to promote industrial intelligence, resilience, and data-driven decision-making. In this respect, the research objectives are developed to offer a systematic search of the world research patterns, determine powerful factors, and visualize the new tendencies that stipulate the development of this interdisciplinary direction. The goals are also aimed at providing not only theoretical insights but also practical advice on industries and policymakers to implement integrated technological approaches to make sure that the operation is efficient, cyber secure, and innovative in a long-term perspective [5]. The

proposed study aims to develop a deep insight into the possible alignment between ML, BDA, and Cybersecurity to enhance Industry 4.0 ecosystems and guide future policy and research by conducting a bibliometric and interpretive study.

The study aims to conduct an in-depth analysis of the roles of Machine Learning (ML), Big Data Analytics (BDA), and Cybersecurity within the Industry 4.0 framework, focusing on how these technologies collaborate to drive intelligent, secure, and sustainable transformation in industries. It seeks to explore global research trends, including the growth or decline in publications and citations from 2020 to 2025, offering a clear overview of the developments and key insights in this interdisciplinary field[2]. The research is also aimed at defining the most powerful authors, institutions, nations and publication outlets affecting this sphere with an emphasis on the main collaboration trends and knowledge networking. Moreover, it will be able to map the intellectual framework, thematic areas and emerging research trends to uncover future opportunities of innovation [6]. The study aims to offer both theoretical insights and practical implications that may help industries, researchers and policy makers to build data-driven, secure and resilient industrial ecosystems in line with the aspirations of Industry 4.0 by integrating both bibliometric and qualitative analysis.

The current literature demonstrates there is a significant research gap in the perception of the concept of integrated use of Machine Learning (ML), Big Data Analytics (BDA) and Cybersecurity in the sphere of Industry 4.0. The studies in the majority of the cases analyze these areas individually without comprehensive frameworks to describe the mutual influence and the creation of intelligent, secure, and sustainable industrial systems [7-11]. Studies are still constrained by data heterogeneity, poor governance model, and lack of empirical validation. Ethical, person-centred and policy factors tend to be ignored, and Regional focus limits International inclusivity. Thus, the new research needs to create interdisciplinary and explicable concepts that relate the technological innovation with sustainable, secure and resilient industrial transformation during the digital era [8-13].

To address these gaps, the research aims to answer three core questions:

1) **RQ 1:** How has the research on Machine Learning, Cyber Security and Big Data Analytics in the context of Industry 4.0 evolved over time?

2) **RQ 2:** Who are the most influential authors, institutions, countries and publication sources contributing to this research field?
3) **RQ 3:** What are the main areas of study, new developments and potential paths in Industry 4.0's fields of machine learning, cyber security, and big data analytics?

To respond to our RQ and answer it, we will strive to achieve the three particular objectives:

1) **RO 1:** To analyze the growth trend, output of publications and influence of citations of research on big data analytics, cyber security and machine learning in the era of Industry 4.0.
2) **RO 2:** To identify which authors, organizations, nations and journals have had the greatest impact and productivity in forming this field of study.
3) **RO 3:** To map and interpret the intellectual structure, thematic clusters and emerging research trends to highlight future research opportunities in this field.

2. LITERATURE REVIEW

Industry 4.0 describes the integration of cyber-physical systems, IoT, cloud/edge computing, and data-driven intelligence into manufacturing and service operations [9-11]. This convergence has three integrated pillars. The first one is machine learning used for decision automation and optimization. Second is big data analytics (BDA). It is used to manage and extract value from the massive, heterogeneous data streams produced across the industrial value chain. And third pillar is cybersecurity, aimed to protect the integrity, confidentiality, and availability of connected systems [10]. Recent systematic reviews note that these three are not independent domains. Rather they co-evolve. [8] reported that though ML and BDA enable advanced capabilities, it parallelly increases the attack surface. Thus, new challenges are being created worldwide.

Machine learning has been widely adopted across Industry 4.0 use cases. Mentionable are predictive maintenance, quality control and defect detection, process parameter optimization, anomaly detection for cybersecurity and intelligent robotics [11], [12] and [13]. Reviews map a progression from classical supervised models to deep learning and hybrid approaches. Especially when they have to deal with image, sensor, and time-series data. The literature emphasizes predictive maintenance as the most mature industrial ML

application, driven by time-series modelling and survival analysis variants [14]; [15]. Recent studies note three methodological shifts: (1) migration toward deep learning for high-dimensional sensor and vision data [16], (2) increased interest in online/streaming ML for real-time decisioning at the edge [17] and (3) adoption of explainable and trustworthy ML methods because of regulatory and operational needs [18]. [19] and [20] report that tooling trends show widespread use of ecosystems and edge deployment frameworks that support model quantization and resource-constrained inference. These trends appear across systematic reviews that analyze publication and implementation patterns.

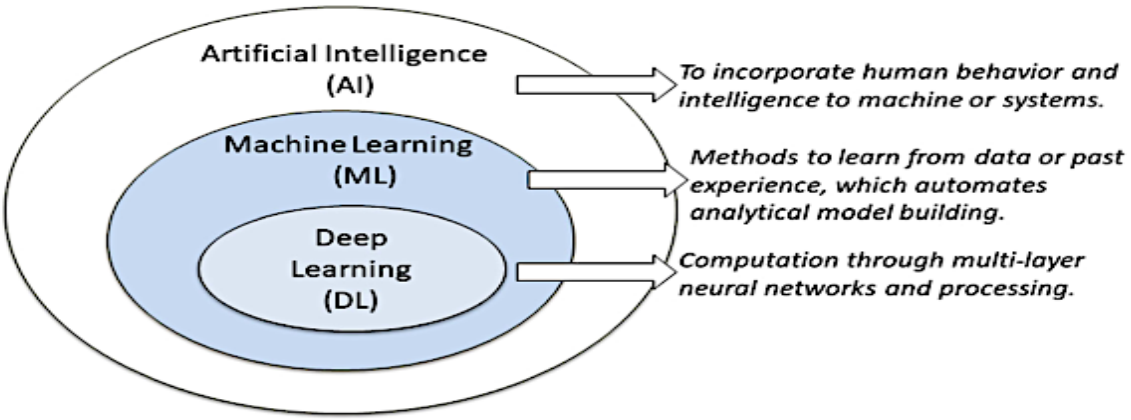

Figure 1. An illustration of machine learning (ML) including deep learning (DL) relative to artificial intelligence (AI).

Big data analytics in Industry 4.0 commonly deploys hybrid cloud–edge architectures: raw high-frequency data are ingested and preprocessed at the edge, summarized to reduce bandwidth, and forwarded to cloud platforms for heavy analytics and historical model training [21]. Platform reviews emphasize distributed storage, stream processing (Kafka, Flink), and data lakes as foundational elements [22]. [23] points that federated and privacy-preserving analytics are growing due to data-sharing constraints across supply-chain partners. The literature demonstrates BDA's role in operational decision support functions like real-time scheduling, demand forecasting, anomaly detection. Role in strategic functions including supply-chain resilience, sustainability metrics were also recognized [24]. Logistics and operations research review reveal a broad set of modeling techniques. Prominent ones are forecasting, optimization and simulation. Their function is often combined with BDA pipelines. This coordination support multi-criteria decisions under uncertainty [25]; [26]. A persistent theme is that data heterogeneity (formats,

sampling rates), missing values, and labeling scarcity limit ML/BDA effectiveness. [27] thus called for unified data ontologies, stronger metadata practices, and governance frameworks. Aim of this was to ensure model reusability and regulatory compliance. These government needs also tie directly to cybersecurity and privacy requirements.

Threats at multiple layers were vulnerable due to the converged systems. Those targeted device/firmware compromise, man-in-the-middle attacks on industrial networks, ransomware that targets OT (operational technology), and ML-targeted exploits (data poisoning, model inversion) [28]. Reviews highlight that legacy industrial control systems (ICS) and protocols lacking authentication are especially vulnerable. Alongside combination of IT and OT expands attacker entry points [29]. Recent literature developed security-by-design approaches, integrating security controls at sensor, edge, and cloud layers [30]. Framework proposals emphasize layered defenses (network segmentation, zero-trust principles), continuous monitoring (IDS/IPS tailored to ICS). Significant other suggestions were use of ML for adaptive intrusion detection. However, caution was advised for ML-based detection systems that themselves need robust evaluation and adversarial-resilience testing [31]. Privacy-preserving analytics (federated learning, differential privacy) are flagged as necessary. Especially in times when cross-firm data sharing is required for improved predictive models. Thus, regulatory pressures (sectoral and regional data laws) are increasingly shaping how BDA and ML can be operationalized in Industry 4.0 contexts [32].

Table 1. A list of Relevant Studies on Emerging Technologies in Industry 4.0

Name of 4.0 Technology	Description	Applications Area	Economic impact	Citation
Machine Learning (ML)	Algorithms that learn patterns from data (supervised, unsupervised, reinforcement, deep learning) to predict, classify, optimize and	Predictive maintenance, quality inspection (vision), process optimisation, anomaly detection, robotics control,	Lowers downtime, improves yield and throughput, reduces costs of inspection and maintenance; enables new data-driven business models.	[11]; [12] and [13]

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Name of 4.0 Technology	Description	Applications Area	Economic impact	Citation
	automate decisions.	adaptive scheduling.		
Big Data Analytics (BDA)	Ingestion, storage, processing and analysis of large, heterogeneous industrial datasets (telemetry, logs, images, transactional). Includes stream processing, data lakes and advanced analytics.	Real-time decision support, demand forecasting, supply-chain optimisation, capacity planning, KPI dashboards.	Improves accuracy, reduces inventory/stockouts, increases operational agility and can produce measurable cost savings across the value chain.	[21]; [22] and [23]
Cybersecurity for Industry 4.0	Practices and technologies (network segmentation, IDS/IPS, secure OT/ICS, zero-trust, ML-based detection) to protect interconnected cyber-physical systems.	ICS/OT protection, intrusion detection, secure firmware/endpoint management, supply-chain security and incident response.	Prevents costly outages and ransomware losses; protects IP and safety—investment yields large avoided-loss benefits but rising threat levels increase compliance and insurance costs.	[28] and [29]
Digital Twin	Live, virtual replica of an	Predictive maintenance,	Shortens commissioning	[33]

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Name of 4.0 Technology	Description	Applications Area	Economic impact	Citation
	asset, process, or system fed by real-time data used for monitoring, simulation, optimisation and what-if analysis.	process optimisation, design validation, layout planning, virtual commissioning.	cycles, reduces unplanned downtime, improves design and operational efficiency — can materially lower lifecycle costs of assets.	
Internet of Things (IoT)	Network of connected sensors/actuators and gateways that produce continuous telemetry enabling visibility and remote control of physical assets.	Asset tracking, environmental sensing, machine health monitoring, smart logistics and energy management.	Enables transparency across operations and supply chains, reduces waste and inventory losses, and supports new service revenues (e.g., outcome-based contracts).	[34]
Collaborative Robots (Cobots) / Advanced Robotics	Robots designed to safely work alongside humans (force-limiters, vision, intuitive programming), often with embedded sensing and AI	Assembly, packing, inspection, machine tending, logistics, small batch/custom manufacturing.	Lowers entry cost for automation in SMEs, increases labor productivity and flexibility; can shift workforce roles rather than wholesale displacement.	[35]

Name of 4.0 Technology	Description	Applications Area	Economic impact	Citation
	for flexible automation.			
Blockchain (for Supply-Chain & Data Integrity)	Distributed ledger technology applied to provenance, immutable record keeping, and trusted multi-party workflows; often combined with IoT for traceability.	Product provenance, anti-counterfeiting, supplier auditing, secure data-sharing agreements.	Improves traceability and trust between partners, can reduce dispute costs and fraud losses; adoption depends on integration costs and governance.	[36]

3. METHODS

3.1. Materials and methods

This research adopts a hybrid research paradigm, which involves a combination of quantitative analysis using bibliometrics and qualitative analysis and interpretation using texts. It uses secondary data source such as Scopus database to give an in-depth analysis of the patterns, trends and thematic developments in the field of research. This paper seeks to critically analyze and trace the new trends and major changes in and the future directions of Machine Learning, Cybersecurity and Big Data Analytics in the context of Industry 4.0.

3.2. Bibliometric analysis

Bibliometric analysis is one of the long-established quantitative approaches, which systematically converts large and unsystematic academic literature into structured and measurable information. This method allows researchers to discover the conceptual

background, intellectual relationships, and the development of the research in the field of science [37]. Besides the measures of articles published per year, citations, the collaboration pattern and most active authors, institutions and countries, a bibliometric analysis is especially relevant when it comes to determining the trends and hotspots of a particular field [38].

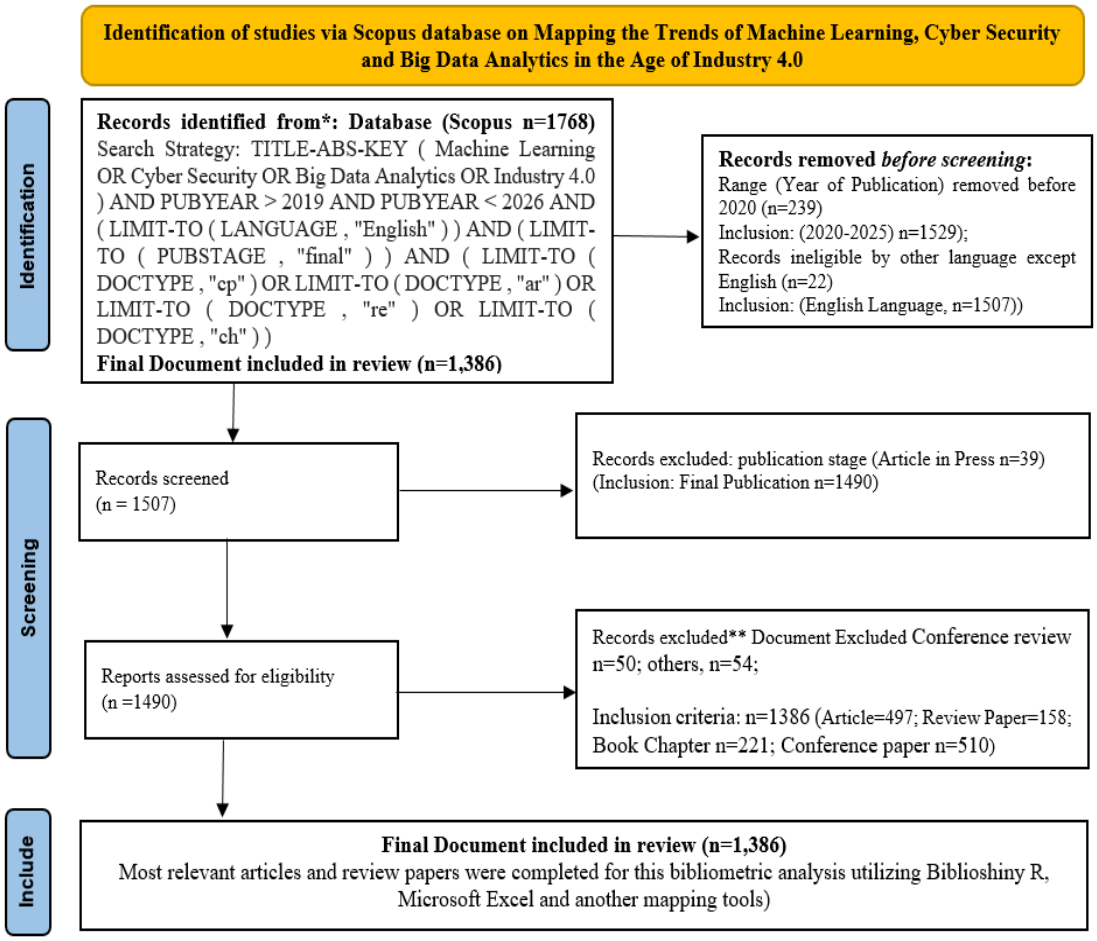

Figure 2. PRISMA based Scopus Indexing Methodology

3.3. Selection of database and search strategy

Figure 2 shows the methodological approach used to search and filter useful articles in the Scopus database to trace the research trend in the topics of Machine Learning, Cyber Security and Big Data Analytics in the sphere of Industry 4.0. To evaluate the quality of the selected studies, a structured screening process was undertaken by applying preset inclusion and exclusion criteria to select only relevant studies, methodological consistency and overall reliability. The exclusion criteria were used to eliminate the irrelevant or non-conforming researches and the articles that passed through the

inclusion criteria were retained to be analyzed further. Other databases, like Web of Science or the DOAJ indexing database, were not accessible by any of our authors. A preliminary total of 1,768 records were retrieved due to a broad-based search strategy confined to the publication of articles in English language between 2020 and 2025. Non-English publications lacked co-authors and even translators. Thus, this study included only articles available in English. After filtering the 239 studies that were out of the publication date and 22 non-English documents, 1507 records were left to be screened. Among them, 39 papers and 1,490 eligible records were excluded, and 1,490 records were selected and assessed in detail. Another narrowing was done, where 104 documents were removed including 50 conference reviews and 54 other irrelevant papers. As a result, 1,386 records were completed in bibliometric analysis and included 497 research articles, 158 review articles, 221 book chapters and 510 conference papers. Table 1 presents the inclusion and exclusion criteria along with the exact search parameters in a systematic way.

Table 2. Search criteria, inclusion and exclusion criteria

Keywords	Search Strategy: TITLE-ABS-KEY (Machine Learning OR Cyber Security OR Big Data Analytics OR Industry 4.0) AND PUBYEAR > 2019 AND PUBYEAR < 2026 AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (PUBSTAGE , "final")) AND (LIMIT-TO (DOCTYPE , "cp") OR LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE , "re") OR LIMIT-TO (DOCTYPE , "ch"))	
Criteria	**No. of inclusion**	**No. of exclusion**
Publication Stage	Final Publication Inclusion n=1,490	Final Publication exclusion n=39
Document Types	Peer- reviewed articles (Articles n=497; Review Paper n=158; Book Chapter n=221; Conference paper n=510)	Record excluded except Conference review n=50; Others, n=54
Timespan	2020-2025	
Language	English	
Final Selection	1,386	

3.4. Data cleaning and analysis

The Scopus was chosen as the main database in terms of data collection due to an extended multidisciplinary coverage and the selection of high-quality and peer-reviewed articles. The retrieved bibliographic records were exported in Comma-Separated Values (CSV) file and pre-processed in Microsoft Excel to provide concreteness data and eliminate redundancy. The filtered data was subsequently inputted into Biblioshiny, the web-based interface of the R package Bibliometrix, to perform advanced bibliometric and visualization analysis *[39]*. Modern research has been well-informed of Biblioshiny as an easy-to-use platform, which offers powerful analytical tools and is efficient in visualizing scientific networks and theme changes *[40]*; *[41]*.

4. RESULTS AND DISCUSSION

4.1. Bibliometric Data Collection Overview

As seen in table 3, the bibliometric data analyzed between 2020 and 2025 gives an overview of the data. It contains 1,386 entries comprising of 466 journals and books, at an annual growth rate of 7.09. The dataset is made up of 11,311 references with an average of 24.98 references per document and average age of the document of 2.26 years. In this collection, 5,033 authors are involved, including 95 single-authored ones. The rate of international co-authorship is 28.28 which means that there is a moderate global collaboration. Data also shows that the preponderance of journal articles (497) and conference papers (510), then book chapters (221) and reviews (158) is predominated.

Description	Results
MAIN INFORMATION ABOUT DATA	
Timespan	2020:2025
Sources (Journals, Books, etc)	466
Documents	1386
Annual Growth Rate %	7.09
Document Average Age	2.26
Average citations per doc	24.98
References	11311
DOCUMENT CONTENTS	
Keywords Plus (ID)	6512

Author's Keywords (DE)	3299
AUTHORS	
Authors	5033
Authors of single-authored docs	95
AUTHORS COLLABORATION	
Single-authored docs	101
Co-Authors per Doc	4.04
International co-authorships %	28.28
DOCUMENT TYPES	
article	497
book chapter	221
conference paper	510
review	158

4.2. Descriptive analysis

4.2.1. The trend in publication and increase in articles

Figure 3 shows the trend in the annual publication between 2020 and 2025, which can be seen to have a generally increasing trend in the number of articles published annually. The publications started to grow in 2020 and peaked in 2024 to reach 295 and then slightly decreased to 231 in 2025. This trend indicates that there is a rising research interest in the area and there may be occasional fluctuations that may be connected to outside of the research area (i.e. research funding, world events or publishing patterns). The ongoing increase until 2024 demonstrates an increased academic interest and performance.

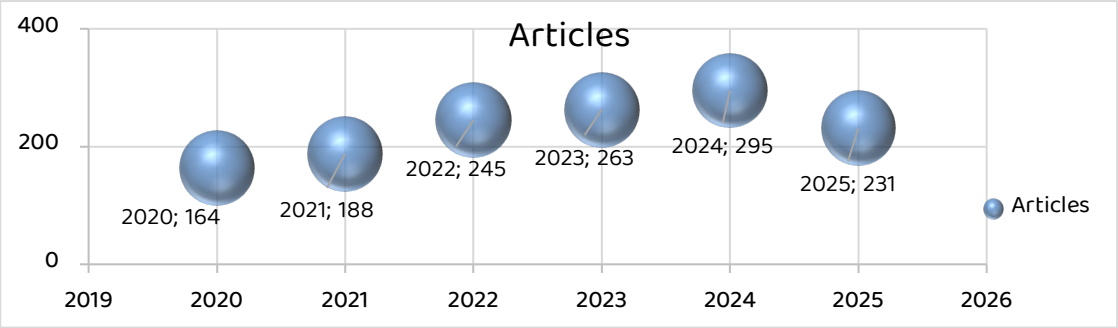

Figure 3. Trends and annual publication

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

4.2.2. Working in an author cluster

This network visualization presents the co-authorship network of the most prolific or centrally connected authors in the research area studied in figure 4. The nodes are individual authors and the size of a node is dependent on the overall publication output of a particular author or the number of co-authorship links (often called strength). The edges between the nodes show collaboration links and the thickness of the line is usually shown using the frequency or strength of co-authorship between the two connected authors.

The network is described as having several discrete clusters, each of them being outlined by a various color (e.g., red, green, blue). This clustering indicates that the research collaboration in this sector is highly concentrated in a few small research groups or communities, and there are not so many bridge links among the large clusters. The central authors in their respective clusters show high degree of cooperation with the members of their immediate group, which signifies the presence of high internal cohesiveness. On the other hand, the peripheral authors or those who have links across clusters (bridge nodes) play a vital role in the inter-cluster flow of knowledge and ideas but are seemingly not very numerous.

Figure 4. Author collaboration cluster

4.3. Publication analysis

4.3.1. Distribution of number of publications by geographical location

Figure 5 locates geographically the distribution of scientific production worldwide by the number of publications with the color changing to dark blue as the output volume increases. It can be observed in the map that the United States, China and India are the most contributing countries, as they are marked with the darkest colors. Production is moderate to high in countries of Western Europe, Canada, Australia and some parts of South America and Southeast Asia. On the contrary, a large part of Africa and Central Asia is painted in the lightest shade, which means that the number of scientific issues is smaller.

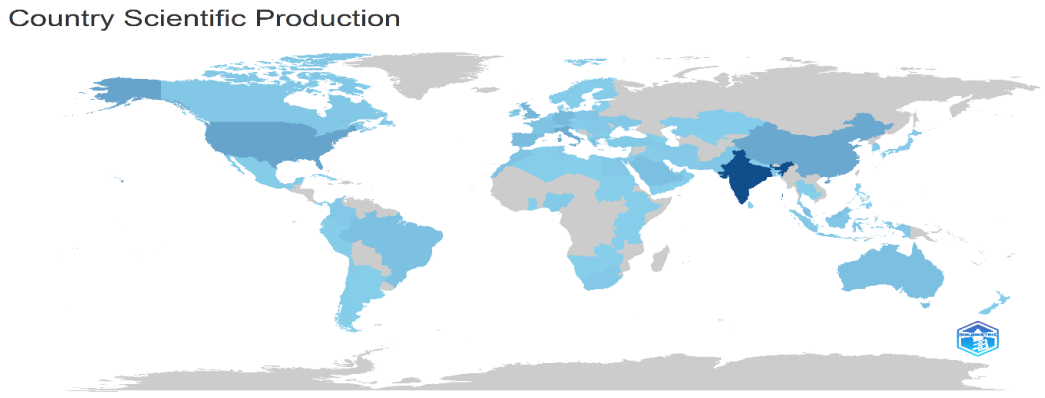

Figure 5. Geographical distribution of number of productions

4.3.2. International Cooperation of Research

Figure 6 shows the international collaboration network in terms of co-authored publications, with each node being a country (or a region). A country node is inversely proportional to its research output or cumulative strength in the area of collaboration. The connecting lines represent collaborative relationships, and lines with more thickness indicate more collaborative relationships between two nations (more papers co-authored). This map demonstrates the geographical arrangement of research partnerships, where countries are grouped into specific collaborative groups (e.g., clusters of countries mostly comprised of Western countries, Asian countries, etc.). The concentration and centrality of some nodes (e.g., the huge central node in the red cluster) demonstrate the presence of a core-periphery structure, with the most powerful and highly connected countries serving as a hub in the international research activity. The general network illustrates that although international cooperation can be observed, it is

often confined to pre-existing geopolitical or economic borders, so a modular network is where the inter-cluster cooperation is not so prominent as the intra-cluster activity.

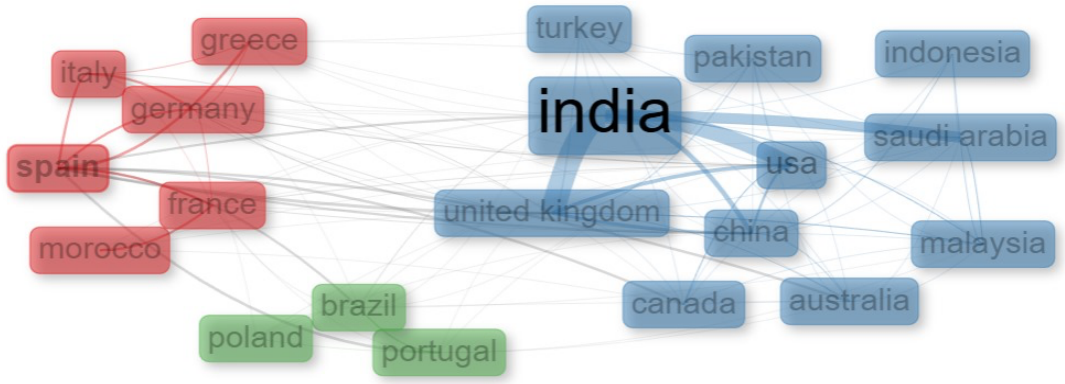

Figure 6. Best joint ventures across nations

4.4. Membership Networks and Keyword Cloud

4.4.1. Most Competent Joint Network

Figure 7 represents the best joint network of institutions, where there are high academic partnerships in the form of multi-polar network. Three central nodes Lovely Professional University, Uttaranchal University and King Khalid University are the key nodes in this network, which make the core of the network. These institutions have affiliations with a number of other smaller, regional partners, including Chitkara University, Alliance University and Nirma University. It is also a worldwide network, showing a variety of diversified partnerships, geographically distributed, in India, Middle East and Europe, linking clusters which comprise the University of Galway and University of Limergan, Hassan II University of Casablanca and Politecnico di Torino and University of Patras.

Figure 7. Most competent joint network

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

4.4.2. Keyword Cloud

Figure 8 is a Keyword Cloud outlining the main themes of the literature with the largest word size being the most frequent. The most prevalent themes that constitute the nucleus of the research are industry 4.0, internet of things, machine learning and artificial intelligence, which confirms that the focus is on advanced manufacturing, connectivity and computational intelligence. The major secondary themes are big data, deep learning and cybersecurity, which describe the range of technologies in the field.

Figure 8. Keyword Cloud

4.5. Citation analysis

The Table 4 consists of the Top 10 most impactful papers based on their citation performance metrics, which presents the major information about the works that shaped the field. Sarker (2021) in SNComputSci is obviously the impactful one, having 1954 Total Citations and the citation velocity of $390.80 TC/Yr. The article that had the highest impact is Ozemel (2020) in J Intell Manuf that has 1586 Total Citations. The reason is that the TC per Year and Normalized TC values are high throughout the board and especially in the top five papers (all having above 600 total citations), which indicates the rapid expansion and relevance of studies in this field. The fact that Sarker (2021) has published several papers indicates a highly active and highly cited writer with a background of work in the field.

Table 4. Top 10 papers

No.	Paper	DOI	Citations	TC /Year	Normalized TC
1	SARKER, 2021, SN COMPUT SCI	10.1007/s42979 -021-00815-1	1954	390.80	36.76

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

No.	Paper	DOI	Citations	TC /Year	Normalized TC
2	OZTEMEL, 2020, J INTELL MANUF	10.1007/s10845-018-1433-8	1586	264.33	27.47
3	QADRI, 2020, IEEE COMMUN SURV TUTOR	10.1109/COMST.2020.2973314	718	119.67	12.43
4	MIHAI, 2022, IEEE COMMUN SURV TUTOR	10.1109/COMST.2022.3208773	700	175.00	22.67
5	JAVAID, 2022, SUSTAIN OPER COMPUT	10.1016/j.susoc.2022.01.008	651	162.75	21.08
6	OSTERRIEDER, 2020, INT J PROD ECON	10.1016/j.ijpe.2019.08.011	408	68.00	7.07
7	KAKANI, 2020, J AGRIC FOOD RES	10.1016/j.jafr.2020.100033	396	66.00	6.86
8	IVANOV, 2021, INT J PROD RES	10.1080/00207543.2020.1798035	378	75.60	7.11
9	SARKER, 2021, SN COMPUT SCI-a-b	10.1007/s42979-021-00557-0	376	75.20	7.07
10	SARKER, 2021, SN COMPUT SCI-a	10.1007/s42979-021-00765-8	366	73.20	6.88

4.6. Production of conceptual structure thematic map

Figure 9 is the conceptual framework of the research area, which is usually based on co-occurrence analysis of keywords (author keywords and/or Keywords Plus). The nodes are the important terms or concepts and the closeness of the nodes indicates that the terms are commonly used in the same publications meaning that there is a good relationship between the themes. The ideas are organized in separate groups (colored, e.g., red, green, blue), which are the key research sub-domains or thematic clusters of the field. The nodes are proportional to the amount of times that the node has occurred in the data. The examination of this map can be used to identify the existing research streams (large, dense clusters) and new themes (smaller, more peripheral nodes). The central concepts that serve as bridges between the clusters are fundamental or interdisciplinary concepts that are essential and connect various sub-domains. The pronounced grouping proves the presence of the specialized spheres of research, whereas the intensity of relations reflects the degree of the thematization and concentration in each sphere.

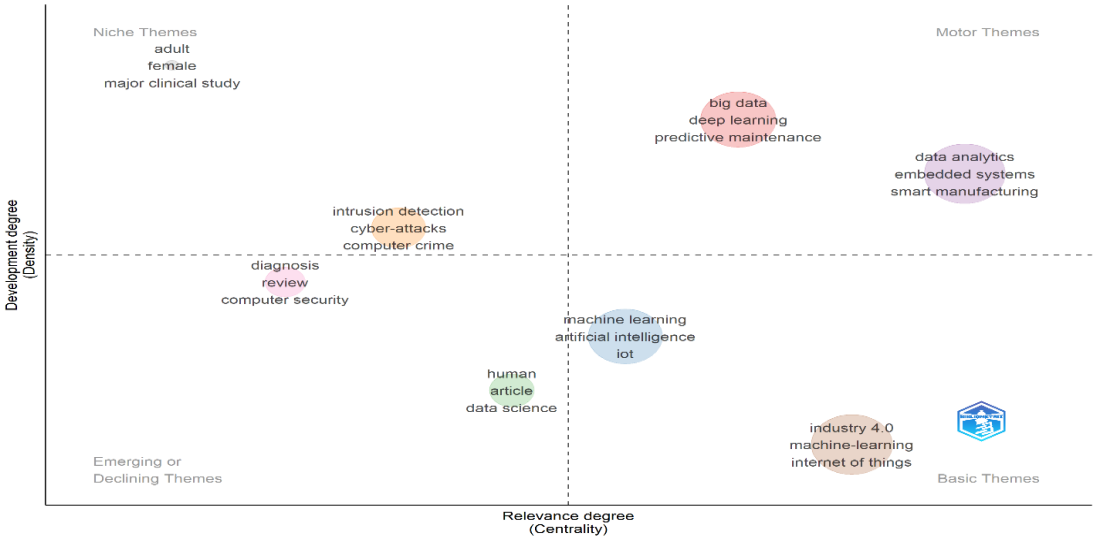

Figure 9. Conceptual structure map

4.7. Discussion

The intersection and integration of the Big Data Analytics (BDA), Machine Learning (ML) and Cyber Security are the essential aspects of the Fourth Industrial Revolution (Industry 4.0). The primary goal will be to examine the growth rate, the productivity of publication and the impact of the research on big data analytics, cyber security and machine learning in the industry 4.0 environment [42]. The foundation of this change lies in the universal use of the Internet of Things (IoT) sensors and Cyber-Physical Systems (CPS) that

generate data volumes that are both high-frequency and multi-dimensional. The critical processing layer BDA is the one that is utilized to bundle and structure this complex data stream into workable input. Besides offering a more efficient operational ecosystem, this integrated data ecosystem is also an expanded and multifaceted attack frontier that needs sophisticated protection [43].

The size of the industrial operation technology (OT) environment and its interconnectedness necessitate a paradigm change of an approach of cybersecurity grounded on ML. This is to determine the authors, organizations, countries and journals that have proved to be the most effective and fruitful in defining this area of study. The conventional, signature-based means of defense has not been adequate to deal with the dynamic threat environment and zero-day attacks that are attributes to modern industrial control systems (ICS) [44]. BDA platforms provide a comprehensive and continuous context that supports both supervised and unsupervised learning methods for real-time anomaly detection, modeling user and device behavior, and delivering proactive threat intelligence. This is essential for ensuring the integrity and availability of critical infrastructure, transforming cybersecurity into a dynamic, adaptive, and predictive security posture vital for long-term operations.

While the effectiveness of these technologies has been demonstrated, their application is still evolving. The study aims to map and clarify the intellectual framework, thematic clusters, and emerging research trends in this field, thereby highlighting future research opportunities[45]. Additionally, the quality of data issue may also decrease the effectiveness of ML, absence of labeled and high-fidelity threat data in industrial systems and the black box approach to deep learning models. This confusion is undesirable to incident response, as the autonomous threat classifications are poorly comprehended by security analysts. To overcome these aspects, there arises the need to filter the data using domain knowledge and do extensive preprocessing of the data so as to ensure the reliability of models

The further research then must lay an emphasis on the development of more trustful and open AI-controlled defense [46]. The most significant part of the confidence in the operator and the ability to ensure the validity of the responses of the security AI is future research of Explainable AI (XAI) to industrial security. There is also a concern to

work out at the critical level the engineering of the ML models that are robust to a form of adversarial attacks, where threat actors are intentionally manipulating the input data to bypass the detection mechanisms. Finally, safe and cross-industrial data-sharing systems should also be guaranteed. Such collaborative models of intelligence will be useful in harnessing the combined knowledge and ensuring sustainable security and resiliency will be able to realize the full potential of the Industry 4.0 era.

The research relies mostly on the secondary data sources and bibliometric analyses as the main sources; though they are useful in mapping the research trends, they might limit the theoretical exploration. Such dependence restricts the ability to develop or experiment with new interdisciplinary models to combine Machine Learning (ML), Big Data Analytics (BDA) and Cybersecurity into Industry 4.0 [47]. Therefore, the research describes but does not offer a complete explanation of technological convergence. The lack of primary data or empirical validation limits the construction of strong theoretical models that would be able to cause, interact or evolve between the technologies. Consequently, some of the conceptual connections, including the dependence between the data-driven intelligence and safe automation, might have not been developed yet, providing an opportunity to be refined theoretically in the future.

The paper can be useful to industries that want to deploy Machine Learning, Big Data Analytics, and Cybersecurity as part of the Industry 4.0 ecosystem. Nevertheless, the use of secondary data constrains its practical application in a real-world industry. As a matter of fact, to implement such technologies successfully, organizations need to consider the readiness of the infrastructure, the interoperability, and the skill gap in the workforce. The industries, technology providers and research institutions will need to collaborate to work on the theoretical insights and convert them into workable solutions. Increasing cross-sector relationships may improve the diffusion of innovations, standardization, and decrease the implementation risks [48]. Furthermore, the pilot projects based on collaboration and collective training programs can spur the digital transformation, so that the theoretical models might be converted into practical industrial strategies.

The leadership preparedness, strategic vision, and management of organizational change are other managerial issues which are not given much focus in the study. In the absence of such considerations, the findings might not provide much practical guidance to

executives who will need to lead the efforts of digital transformation. Also, the research under-investigates workforce training, employee engagement, and upskilling strategies, essential in sustainable implementation [49]. This hinders the formulation of viable managerial models to integrate ML, BDA and Cybersecurity in practice. As a result, decision-makers might be left without the direction they need to develop adaptive leadership models, more and more culture of innovation, and synchronization of human capital development with changes in technology.

The rapid development of Industry 4.0 technologies leads to the rapid obsolescence of the findings of the study because new tools and systems are released. The combination of ML, BDA and Cybersecurity poses the never-ending challenges of interoperability, scalability and technological obsolescence that the research under consideration fails to tackle in a comprehensive manner [50]. Furthermore, the absence of a live assessment of the changing platforms and infrastructures can cause lapses in the knowledge of constraints in practical deployment. Technological upheavals, including the emergence of generative AI or edge computing or quantum security, may change the dynamics depicted in the study considerably.

Policy considerations are mentioned only briefly in the study and leave a significant gap in the knowledge about regulatory and governance aspects of Industry 4.0 technologies. The cross-border data flows, privacy of data, compliance with cybersecurity, intellectual property and cross-border data flows are not studied thoroughly [51]. Also, the differences between the legal frameworks and government support mechanisms are not analyzed in detail, which limits the contribution of the study to the development of the global policy. Lack of detailed policy recommendations can cripple organizations and policymakers in formulating strong systems of governance to adopt the technology safely and ethically. Therefore, the work on the regulation policy in the future should be aimed at its integration to innovation and risk management goals.

Educational aspects, especially workforce preparedness, technical skillfulness, and curriculum development are poorly covered in the research. With the changing of industry 4.0 technologies, a flexible and trained workforce is highly needed. Nonetheless, the insufficient emphasis on the analysis of the skill gaps, training approaches and the academic-industrial partnership restricts the contribution of the artwork to the discourse

of capacity-building. In the absence of clear educational structures, institutions might find it difficult to match the programs to emerging new technological needs resulting in the lack of appropriate skills within the labor market [52]. That is why it becomes extremely important to create systematic educational patterns and lifelong learning programs to equip the professionals with the changing digital ecosystem.

4.8. Limitations & Future Directions

Even though the study provides valuable bibliometric information, it has a number of limitations, which can affect the extent to which the study can be understood and generalized. The study uses only the Scopus database, which, despite its scale, does not cover the relevant publications of other databases, including Web of Science, IEEE Xplore, and SpringerLink, which may lead to the limitation of the diversity of the data set [53]. The time frame (2020-2025) limits the longitudinal approach to the interpretation of the technological development of Industry 4.0 and can exclude previous works foundational to it or the latest innovations that have occurred after 2025. Moreover, the research is limited to the English-language publications, which adds linguistic bias and lowers the global representativeness, especially by non-English-speaking areas [54]. In terms of methodology, the study is focused on the quantitative bibliometric methodology that might be deprived of a contextual interpretation and could not reflect the qualitative layer of the technological, managerial, and social implications. The lack of the experimental confirmation or the case studies conducted in the industry hinder the practical applicability of the study. Also, the study does not represent small and medium-sized enterprises (SMES) and developing regions as this restricts inclusivity in the scales of industries and geographical areas [55]. Lastly, the data visualization tools used in the study are too static therefore the dynamics and changing nature of Industry 4.0 interactions which can solely be attained through adaptive, cross-disciplinary and real-time analytical tools are not completely reflected in the study hence the need to carry out future research using these tools.

The current literature is mainly focused on the Industry 4.0 trends at a singular time, providing no more than the picture of the integration but not a whole picture of its development. This limits the insight into the way the Developing phase and maturity of Big Data Analytics (BDA) and Cybersecurity are developing in parallel with other industries [56-58]. As a result, the long-term viability, performance gains and strategic versatility of

these technologies are poorly evidenced. Future Direction Future studies will use longitudinal and mixed method designs to track the continued implementation, change, and interdependence of ML, BDA and Cybersecurity on a longer-term basis. These researches will present a dynamic perception of technology adoption, determine the phase of technological maturity and mention the emerging trends that shape the technological lifecycle of Industry 4.0.

The current literature tends to approach Industry 4.0 as a generic principle but ignores the specific needs, problems, and implementation in different industries. This generalization spoils the applicability of results and the creation of tailor-made digital strategies. Lack of industry expertise makes it difficult to integrate effectively in industry like manufacturing, logistics, healthcare and energy. Future Direction Future research will involve in-depth empirical research on particular industrial sectors in order to identify contextual adoption barriers, sector level of readiness, and best practice. These specific analyses will allow researchers and practitioners to come up with frameworks that correspond to the level of complexity of operations of an industry, its regulatory environment and technological base.

Most of the literature available today is conceptual and technological based instead of practical deployment issues. The readiness of the organization, competency of the workforce, cost implications and challenges in scaling are not adequately addressed. This leads to lack of congruence between theory and practice in industry hence constrained actionable knowledge to the decision makers. Future Direction Future research will focus on the investigation of practical integration frameworks that will focus on the implementation feasibility[59-60].

Although Industry 4.0 encourages the use of connectivity and automation, a great number of researchers ignore the growing complexity of cybersecurity threats and the necessity to ensure a resilient system that can adapt to changing conditions. There is scanty literature on dynamic threat mitigation, real time defense or development of intelligent systems that can self-repair and adapt to cyber pressure. Future Direction: The authors will investigate how to design adaptive, secure, and intelligent Industry 4.0 ecosystems to autonomously react to the changing cyber threats and operational disruptions.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

The fast-changing technological transformation that is the Industry 4.0 has pushed ahead of the creation of parallel systems of regulation, ethics and education. The gaps that exist include the absence of holistic policies to regulate the sharing of data, digital ethics, and compliance with cybersecurity standards and there is no adequate focus on the alignment of education and training programs in line with new digital skills requirements. Future Direction Future studies will focus on formulating combined policy systems and learning frameworks that facilitate safe, ethical and competent digital change.

5. CONCLUSION

The analysis of the research trends of the Machine Learning, Big Data Analytics, and Cybersecurity in Industry 4.0 between 2020 and 2025 through mapping shows that the research trends in the field experienced a 7.09 percent annual growth rate and a growing global attention. It is dominated by the United States, China, and India, and there is a high level of cooperation between Europe and Asia. The major areas of research are digital twins, deep learning, predictive maintenance, and IoT, which represent the transition to the use of AI-based, data-intensive systems as opposed to traditional automation. Although cybersecurity will guarantee the protection of the systems, ML and BDA will help in automation and decision-making. Further studies need to go beyond bibliometric analysis to establish comprehensive and empirically validated frameworks that can be used to fill the integration gaps between Machine Learning (ML), Big Data Analytics (BDA) and Cybersecurity in Industry 4.0. The integrate predictive analytics with adaptive security controls, enabling industries to balance automation and protection in real-time. Long-term cross-industry studies are needed to assess the scalability, cost-efficiency, and sustainability of integrated systems. Additionally, computer scientists, engineers, and policymakers must collaborate to create ethical, secure, and efficient governance frameworks. Incorporating experimental case studies, simulations, and AI-based data governance will bridge the gap between theory and practice, fostering a robust and secure Industry 4.0 ecosystem. Future research should focus on creating interdisciplinary frameworks to enable secure, intelligent, and resilient Industry 4.0 environments with privacy-conscious data governance.

ACKNOWLEDGMENT

Authors have acknowledged to Mohammad Rakibul Islam Bhuiyan, Assistant Professor, Begum Rokeya University, Rangpur, Bangladesh, for his guidelines and knowledge support to complete the whole research within short time.

REFERENCES

[1] K. Zhang, Y. Shi, S. Karnouskos, T. Sauter, H. Fang, and A. W. Colombo, "Advancements in Industrial Cyber-Physical Systems: An Overview and Perspectives," *IEEE Trans. Ind. Inform.*, vol. 19, no. 1, pp. 716–729, Jan. 2023, doi: 10.1109/TII.2022.3199481.

[2] R. Iqbal, F. Doctor, B. More, S. Mahmud, and U. Yousuf, "Big data analytics: Computational intelligence techniques and application areas," *Technol. Forecast. Soc. Change*, vol. 153, p. 119253, Apr. 2020, doi: 10.1016/j.techfore.2018.03.024.

[3] B. I. Adekunle, E. C. Chukwuma-Eke, E. D. Balogun, and K. O. Ogunsola, "Machine Learning for Automation: Developing Data-Driven Solutions for Process Optimization and Accuracy Improvement," *Int. J. Multidiscip. Res. Growth Eval.*, vol. 3, no. 1, pp. 800–808, 2021, doi: 10.54660/.IJMRGE.2021.2.1.800-808.

[4] M. Ghobakhloo, M. Iranmanesh, A. Grybauskas, M. Vilkas, and M. Petraitė, "Industry 4.0, innovation, and sustainable development: A systematic review and a roadmap to sustainable innovation," *Bus. Strategy Environ.*, vol. 30, no. 8, pp. 4237–4257, Dec. 2021, doi: 10.1002/bse.2867.

[5] B. Bajic, A. Rikalovic, N. Suzic, and V. Piuri, "Industry 4.0 Implementation Challenges and Opportunities: A Managerial Perspective," *IEEE Syst. J.*, vol. 15, no. 1, pp. 546–559, Mar. 2021, doi: 10.1109/JSYST.2020.3023041.

[6] I. Ahmed, G. Jeon, and F. Piccialli, "From Artificial Intelligence to Explainable Artificial Intelligence in Industry 4.0: A Survey on What, How, and Where," *IEEE Trans. Ind. Inform.*, vol. 18, no. 8, pp. 5031–5042, Aug. 2022, doi: 10.1109/TII.2022.3146552.

[7] A. Amin et al., "The Adoption of Industry 4.0 Technologies by Using the Technology Organizational Environment Framework: The Mediating Role to Manufacturing Performance in a Developing Country," *Bus. Strategy and Development*, vol. 7, no. 2, Apr. 2024, doi: 10.1002/bsd2.363.

[8] J. Yu, A. V. Shvetsov, and S. Hamood Alsamhi, "Leveraging Machine Learning for Cybersecurity Resilience in Industry 4.0: Challenges and Future Directions," *IEEE Access*, vol. 12, pp. 159579–159596, 2024, doi: 10.1109/ACCESS.2024.3482987.

[9] M. R. Bhuiyan et al., "The Mediating Effect of Innovation Capabilities, Information Quality and Supply Chain Resilience in the Relationship between Big Data Analytics Capability (BDAC) and Healthcare Performance," *SAGE Open*, vol. 15, no. 3, Jan. 2025, doi: 10.1177/21582440251362262.

[10] M. Singh, R. Goyat, and R. Panwar, "Fundamental pillars for industry 4.0 development: implementation framework and challenges in manufacturing environment," *TQM J.*, vol. 36, no. 1, pp. 288–309, Jan. 2024, doi: 10.1108/TQM-07-2022-0231.

[11] U. Azmaien, "Integrating Artificial Intelligence and Social Media for English as a Foreign Language (EFL) Learning: A Study on Meta-AI's Influence on Reading Comprehension," *J. Inf. Syst. Informatics*, vol. 7, no. 2, Jun. 2025, pp. 1083–1105, doi: 10.51519/journalisi.v7i2.1070.

[12] A. Q. Md et al., "A Review on Data-Driven Quality Prediction in the Production Process with Machine Learning for Industry 4.0," *Processes*, vol. 10, no. 10, p. 1966, Sep. 2022, doi: 10.3390/pr10101966.

[13] E. T. Ogidan, O. P. Olawale, and K. Dimililer, "Machine Learning Applications in Industry 4.0," in *Handbook of Intelligent and Sustainable Manufacturing*, 1st ed., Boca Raton: CRC Press, 2024, pp. 284–304, doi: 10.1201/9781003405870-16.

[14] O. Serradilla et al., "Deep learning models for predictive maintenance: a survey, comparison, challenges and prospects," *Appl. Intell.*, vol. 52, no. 10, pp. 10934–10964, Aug. 2022, doi: 10.1007/s10489-021-03004-y.

[15] C. Tsallis et al., "Application-Wise Review of Machine Learning-Based Predictive Maintenance: Trends, Challenges, and Future Directions," *Appl. Sci.*, vol. 15, no. 9, p. 4898, Apr. 2025, doi: 10.3390/app15094898.

[16] T. Georgiou et al., "A survey of traditional and deep learning-based feature descriptors for high dimensional data in computer vision," *Int. J. Multimed. Inf. Retr.*, vol. 9, no. 3, pp. 135–170, Sep. 2020, doi: 10.1007/s13735-019-00183-w.

[17] Z. Zhang et al., "Advances in Machine-Learning Enhanced Nanosensors: From Cloud Artificial Intelligence Toward Future Edge Computing at Chip Level," *Small Struct.*, vol. 5, no. 4, p. 2300325, Apr. 2024, doi: 10.1002/sstr.202300325.

[18] V. Chamola et al., "A Review of Trustworthy and Explainable Artificial Intelligence (XAI)," *IEEE Access*, vol. 11, pp. 78994–79015, 2023, doi: 10.1109/ACCESS.2023.3294569.

[19] Y. Nimmagadda, "Model Optimization Techniques for Edge Devices," in *Model Optimization Methods for Efficient and Edge AI*, 1st ed., P. R. Chelliah, A. M. Rahmani, R. Colby, G. Nagasubramanian, and S. Ranganath, Eds., Wiley, 2025, pp. 57–85, doi: 10.1002/9781394219230.ch4.

[20] D. Ngo et al., "Edge Intelligence: A Review of Deep Neural Network Inference in Resource-Limited Environments," *Electronics*, vol. 14, no. 12, p. 2495, Jun. 2025, doi: 10.3390/electronics14122495.

[21] I. M. Al Jawarneh et al., "Efficient Parallel Processing of Big Data on Supercomputers for Industrial IoT Environments," *Electronics*, vol. 14, no. 13, p. 2626, Jun. 2025, doi: 10.3390/electronics14132626.

[22] P. Wieder and H. Nolte, "Toward data lakes as central building blocks for data management and analysis," *Front. Big Data*, vol. 5, p. 945720, Aug. 2022, doi: 10.3389/fdata.2022.945720.

[23] X. Tang et al., "Federated graph neural network for privacy-preserved supply chain data sharing," *Appl. Soft Comput.*, vol. 168, p. 112475, Jan. 2025, doi: 10.1016/j.asoc.2024.112475.

[24] J. Rane et al., "Supply Chain Resilience through Internet of Things, Big Data Analytics, and Automation for Real-Time Monitoring," 2025, doi: 10.2139/ssrn.5366936.

[25] H. Jahani et al., "Data science and big data analytics: a systematic review of methodologies used in the supply chain and logistics research," *Ann. Oper. Res.*, Jul. 2023, doi: 10.1007/s10479-023-05390-7.

[26] K. Zekhnini, A. Chaouni Benabdellah, and A. Cherrafi, "A multi-agent based big data analytics system for viable supplier selection," *J. Intell. Manuf.*, vol. 35, no. 8, pp. 3753–3773, Dec. 2024, doi: 10.1007/s10845-023-02253-7.

[27] D. Sargiotis, "Data Governance Frameworks: Models and Best Practices," in *Data Governance*, Cham: Springer Nature Switzerland, 2024, pp. 165–195, doi: 10.1007/978-3-031-67268-2_4.

[28] E. Eugene Schultz, "Risks due to convergence of physical security systems and information technology environments," *Inf. Secur. Tech. Rep.*, vol. 12, no. 2, pp. 80–84, 2007, doi: 10.1016/j.istr.2007.06.001.

[29] M. M. Aslam et al., "Scrutinizing Security in Industrial Control Systems: An Architectural Vulnerabilities and Communication Network Perspective," *IEEE Access*, vol. 12, pp. 67537–67573, 2024, doi: 10.1109/ACCESS.2024.3394848.

[30] V. Casola et al., "Security-by-design in multi-cloud applications: An optimization approach," *Inf. Sci.*, vol. 454–455, pp. 344–362, Jul. 2018, doi: 10.1016/j.ins.2018.04.081.

[31] K. Barik, S. Misra, and L. Fernandez-Sanz, "A Model for Estimating Resiliency of AI-Based Classifiers Defending Against Cyber Attacks," *Int. J. Comput. Intell. Syst.*, vol. 17, no. 1, p. 290, Nov. 2024, doi: 10.1007/s44196-024-00686-3.

[32] M. Zheng, T. Li, and J. Ye, "The Confluence of AI and Big Data Analytics in Industry 4.0: Fostering Sustainable Strategic Development," *J. Knowl. Econ.*, vol. 16, no. 1, pp. 5479–5515, Jul. 2024, doi: 10.1007/s13132-024-02120-7.

[33] S. Lou et al., "Human-Cyber-Physical System for Industry 5.0: A Review From a Human-Centric Perspective," *IEEE Trans. Autom. Sci. Eng.*, vol. 22, pp. 494–511, 2025, doi: 10.1109/TASE.2024.3360476.

[34] G. B. Narkhede et al., "Industry 5.0 and sustainable manufacturing: a systematic literature review," *Benchmarking Int. J.*, vol. 32, no. 2, pp. 608–635, Feb. 2025, doi: 10.1108/BIJ-03-2023-0196.

[35] T. Rijwani et al., "Industry 5.0: a review of emerging trends and transformative technologies in the next industrial revolution," *Int. J. Interact. Des. Manuf.*, vol. 19, no. 2, pp. 667–679, Feb. 2025, doi: 10.1007/s12008-024-01943-7.

[36] M. R. Bhuiyan, "Industry Readiness and Adaptation of Fourth Industrial Revolution: Applying the Extended TOE Framework," *Human Behav. Emerging Technol.*, vol. 2024, no. 1, Jan. 2024, doi: 10.1155/hbe2/8830228.

[37] I. Zupic and T. Čater, "Bibliometric Methods in Management and Organization," *Organ. Res. Methods*, vol. 18, no. 3, pp. 429–472, Jul. 2015, doi: 10.1177/1094428114562629.

[38] P. Thangavel and B. Chandra, "Two Decades of M-Commerce Consumer Research: A Bibliometric Analysis Using R Biblioshiny," *Sustainability*, vol. 15, no. 15, p. 11835, Aug. 2023, doi: 10.3390/su151511835.

[39] M. Aria and C. Cuccurullo, "bibliometrix: An R-tool for comprehensive science mapping analysis," *J. Informetr.*, vol. 11, no. 4, pp. 959–975, Nov. 2017, doi: 10.1016/j.joi.2017.08.007.

[40] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, and W. M. Lim, "How to conduct a bibliometric analysis: An overview and guidelines," *J. Bus. Res.*, vol. 133, pp. 285–296, Sep. 2021, doi: 10.1016/j.jbusres.2021.04.070.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[41] J. A. Moral-Muñoz, E. Herrera-Viedma, A. Santisteban-Espejo, and M. J. Cobo, "Software tools for conducting bibliometric analysis in science: An up-to-date review," *El Prof. Inf.*, vol. 29, no. 1, Jan. 2020, doi: 10.3145/epi.2020.ene.03.

[42] G. Kabanda, "Performance of Machine Learning and Big Data Analytics Paradigms in Cyber Security," in *AI, Machine Learning and Deep Learning*, 1st ed., Boca Raton: CRC Press, 2023, pp. 191–241, doi: 10.1201/9781003187158-17.

[43] I. Aribilola et al., "SuPOR: A lightweight stream cipher for confidentiality and attack-resilient visual data security in IoT," *Int. J. Crit. Infrastruct. Prot.*, vol. 50, p. 100786, Sep. 2025, doi: 10.1016/j.ijcip.2025.100786.

[44] A. Srivastava and D. Sinha, "Fp Growth-Based Zero-Day Attack Signature Extraction & Detection Model for High-Volume Attacks on Real-Time Data Stream," 2024, doi: 10.2139/ssrn.4701527.

[45] A. Jordan and D. Berleant, "Data Science Knowledge and Skills That Reliability Engineers Need: A Survey," in *2023 Annual Reliability and Maintainability Symposium (RAMS)*, Orlando, FL, USA: IEEE, Jan. 2023, pp. 1–6, doi: 10.1109/RAMS51473.2023.10088219.

[46] M. F. E- Alam et al., "The Role of the Three Zero Framework in Advancing Global Sustainable Development through Bibliometric and Text Mining Analysis," *Discover Sustainability*, vol. 6, no. 1, Oct. 2025, doi: 10.1007/s43621-025-01919-x.

[47] P. Ghose et al., "Gravitating towards Technology-Based Emerging Financial Crime: A PRISMA-Based Systematic Review," *Int. J. Innov. Res. Sci. Stud.*, vol. 8, no. 2, Apr. 2025, pp. 3387–3402, doi: 10.53894/ijirss.v8i2.6014.

[48] Y. A. Velásquez Ramos, "Little Attention of Companies in the Commercial Sector Regarding the Implementation of Safety and Health at Work in Colombia During the Year 2015 to 2020," *SCT Proc. Interdiscip. Insights Innov.*, vol. 1, p. 79, Dec. 2023, doi: 10.56294/piii202379.

[49] D. Norman, "Design, Business Models, and Human-Technology Teamwork: As automation and artificial intelligence technologies develop, we need to think less about human-machine interfaces and more about human-machine teamwork," *Res.-Technol. Manag.*, vol. 60, no. 1, pp. 26–30, Jan. 2017, doi: 10.1080/08956308.2017.1255051.

[50] M. Rani, "Never-ending Journey of Platelet Concentrates," *Res. Rev.*, May 2022, doi: 10.52845/CMRO/2022/5-4-1.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[51] E. Laidlaw, "Privacy and Cybersecurity in Digital Trade: The Challenge of Cross Border Data Flows," *SSRN Electron. J.*, 2021, doi: 10.2139/ssrn.3790936.

[52] L. Montenbruck, "Evaluation of Demand-led Vocational Training Programs in Pakistan," doi: 10.1257/rct.7910.

[53] C. Yin, "Which Tasks of Architect Can Computers Perform? A Study Integrating Pattern Language, Linguistics, and Data Types," 2024, doi: 10.2139/ssrn.4995740.

[54] M. C. Murugesh et al., "A Case Study of Additive Manufacturing in Prosthesis Development in Industry 4.0," in *Industry 4.0 in Small and Medium-Sized Enterprises (SMEs)*, 1st ed., Boca Raton: CRC Press, 2022, pp. 109–122, doi: 10.1201/9781003200857-7.

[55] Md. N. Hasan et al., "Enhancing Financial Information Security through Advanced Predictive Analytics: A PRISMA Based Systematic Review," *Edelweiss Appl. Sci. Technol.*, vol. 9, no. 7, Jul. 2025, pp. 2222–2245, doi: 10.55214/2576-8484.v9i7.9142.

[56] Md. I. Pramanik et al., "Emerging Technological Trends in Financial Crime and Money Laundering: A Bibliometric Analysis of Cryptocurrency's Role and Global Research Collaboration," *J. Posthumanism*, vol. 5, no. 6, Jun. 2025, pp. 3611–3633, doi: 10.63332/joph.v5i6.2493.

[57] A. Domenteanu et al., "Mapping the Research Landscape of Industry 5.0 from a Machine Learning and Big Data Analytics Perspective: A Bibliometric Approach," *Sustainability*, vol. 16, no. 7, p. 2764, Mar. 2024, doi: 10.3390/su16072764.

[58] Md. W. Ullah et al., "A Systematic Review on Information Security Policies in the USA Banking System and Global Banking: Risks, Rewards, and Future Trends," *Edelweiss Appl. Sci. Technol.*, vol. 8, no. 6, Dec. 2024, pp. 8437–8453, doi: 10.55214/25768484.v8i6.3816.

[59] Md. A. Islam et al., "Artificial Intelligence in Digital Marketing Automation: Enhancing Personalization, Predictive Analytics, and Ethical Integration," *Edelweiss Appl. Sci. Technol.*, vol. 8, no. 6, Nov. 2024.

[60] Md. D. Hossen, "What Factors Influence the Increasing Dependency on Mobile Banking in Bangladesh? A Quantitative Study in Bangladesh," *Int. J. Religion*, vol. 5, no. 11, Jul. 2024, pp. 4821–4837, doi: 10.61707/pc78be35.