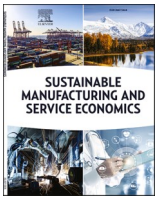
Sustainable Manufacturing and Service Economics 3 (2024) 100018

Contents lists available at ScienceDirect

Sustainable Manufacturing and Service Economics

journal homepage: www.elsevier.com/locate/smse



Full Length Article

A decision support model for assessing and prioritization of industry 5.0 cybersecurity challenges

Ifaz Ahmed [a], Niamat Ullah Ibne Hossain [b,*], Steven A Fazio [c], Marianna Lezzi [d], Md. Saiful Islam [a]

[a] Department of Industrial Engineering and Management, Khulna University Engineering & Technology, Khulna, 9203, Bangladesh
[b] Engineering Management Department, College of Engineering and Computer Science, Arkansas State University, Jonesboro, Arkansas 72467, USA
[c] Department of Industrial and Systems Engineering, Mississippi State University, PO Box 9542, Mississippi State, 39762, USA
[d] Department of Engineering for Innovation, Università del Salento, Campus Ecotekne, Via per Monteroni, 73100, Lecce, Italy

ARTICLE INFO

Keywords:
Cybersecurity
Decision support model
Graph theory and matrix approach (GTMA)
Industry 5.0

ABSTRACT

The world is adopting the Industry 5.0 paradigm to increase human centricity, sustainability, and resilience in efficient, optimized, and profitable manufacturing systems. With benefits, however, come increased risks of economic and physical loss, driving the need for continuous improvement of Industry 5.0 cybersecurity. Implementation and advancement of adequate cybersecurity have created challenges that have been identified in the literature. In this study, key Industry 5.0 cybersecurity challenges and related sub-challenges are highlighted based on a literature review. Graph Theory and Matrix Approach (GTMA) is employed to analyze the challenges and determine relative importance based on permanent values of the variable permanent matrix (VPM). The results identify the most important Industry 5.0 cybersecurity challenges and reveal Industry 5.0 firms should primarily concentrate on supply chain vulnerabilities to decrease data loss and hacking in the organization's supply chain network. This study also recommends that executives and lawmakers acquire knowledge regarding cybersecurity challenges and prepare to deal with them. Addressing these and other subsequently prioritized challenges—the top five rounded out with emergent cybersecurity trends, non-availability of cybersecurity curriculum in education, embedded technical constraints, and absence of skilled employees and training—will lead the methodical development of holistic, robust cybersecurity programs. Firms accepting of this reality may implement such programs to mitigate evolving cyber-risk towards harnessing and sustaining the benefits of novel Industry 5.0 technologies.

1. Introduction

The progression of industry has been marked by different evolutionary leaps in technological progression, including the harnessing of energy from steam, electrification, computerization, and automation of machinery itself. The changes to human civilization that followed these advancements are known as industrial revolutions. The fifth industrial revolution, or I5.0, is the most recent characterized by the symbiosis of human and machine in which networked automation benefits merge with resilience and sustainability in production systems to promote both prosperity and sustainability [1,2]. Increasing awareness of this potential is leading to the prioritization of Industry 5.0 (I5.0) topics in research [3,2]. The technological foundation of Industry 5.0 is linked to the I5.0 Internet of things (IoT), artificial intelligence (AI), Industrial Internet, Interconnected series, and Cyber-physical systems [4]. Industry 5.0 widens the scope of requirements to include revolutionary supply chain changes through increasing resilience, profitability, efficiency, flexibility, and horizontal integration (Tiwari, 2021; [5,6]).

The same Industry 5.0 pathways that enable the integration of advanced smart manufacturing technologies vastly expand the potential for malicious system intrusion. Cybersecurity breaches can result in massive negative impacts such as economic damage, loss of production, injury, and even death [7]. As the rate and severity of cyber-attacks increase, the challenges facing cybersecurity professionals are becoming more and more difficult [8]. In March 2016, terrorists using cellular modems hacked the computer-based operation of a dam in New York [9]. A cyber-attack on Ukrainian power production in 2015 led to the loss of electricity for 225,000 consumers and multiple blackouts [9].

* Corresponding author.
E-mail address: nibnehossain@astate.edu (N.U.I. Hossain).

https://doi.org/10.1016/j.smse.2024.100018
Received 28 February 2023; Received in revised form 6 September 2023; Accepted 24 January 2024
Available online 28 January 2024

Another cyber-attack on a Garman steel plant in 2014 resulted in massive physical damage to the whole manufacturing system [9]. Cyber-attacks had affected two-thirds of Germany's industrial businesses as of 2018. The strain on companies created by data theft, industrial espionage, and sabotage may range from mild to existential. All these situations share two main aspects: (i) the intensive use of smart devices, wireless sensor networks, internet protocols, or cloud and data analytics technologies [10,11,12]; (ii) employees' insufficient awareness in the field of cybersecurity that increases the likelihood of successful cyber-attacks ([13]; Moti et al., 2022).

As modern manufacturing organizations embrace the benefits of Industry 5.0, it is necessary to create robust cybersecurity programs that improve awareness of cybersecurity issues and mitigate the risks of cyber-attacks [7]. In fact, according to Malatras et al. [14], the adoption of appropriate cybersecurity awareness plans could play a key role in providing employees with basic cybersecurity training (e.g., for the most prevalent cyber threats, security requirements are observed, international guidelines are known, and corporate cybersecurity procedures are followed). Implementation of such programs, however, comes with a core group of challenges. In general, exerting effective influence does not only mean informing people about what they should or should not do. People must first acknowledge that information is relevant, understand how to respond, and be willing to accept the results [15]. According to the study conducted by Khando et al. [16], methods for designing engaging and appropriate cybersecurity awareness materials are very often lacking; likewise, various behavioral factors that could increase cybersecurity awareness are often not taken into account. Some employees complain that cybersecurity training programs are too general and not relevant to the tasks performed within their organization [17]. The goal of this study is to analyze the current cybersecurity challenges (and related sub-challenges) facing organizations embracing Industry 5.0. The following research questions will be addressed in this study:

Question 1: What are the current core challenges of Industry 5.0 cybersecurity identified in the literature?
Question 2: What is the relative importance structure of Industry 5.0 cybersecurity challenges?
Question 3: How can a model of the current challenge climate be constructed to enable effective, strategic implementation of cybersecurity programs?

This study utilizes graph theory and matrix approach (GTMA) to analyze the challenges facing Industry 5.0 cybersecurity. GTMA, like many multi-criteria decision-making (MCDM) methods, affords decision makers both method and logic for approaching complex decision systems where optimization of one variable sub-optimizes one or more others [18]. Using GTMA to analyze the cybersecurity challenges facing Industry 5.0 firms brings a holistic perspective lacking in other approaches. This study presents an analysis of survey data collected from industry experts where interrelationships between variables are considered through the GTMA approach. The output is a hierarchical structure of identified challenges; therefore, the objectives of this study are as follows:

- Identify the primary challenges related to Industry 5.0 cybersecurity.
- Determine the ranking among the challenges using GTMA.
- Provide recommendations regarding critical aspects of Industry 5.0 cybersecurity.

Display the efficacy of the GTMA approach in the context of Industry 5.0 related challenges.

The rest of the study is outlined as follows: Section 2 provides general background information and context for cybersecurity in the Industry 5.0 paradigm as well as related works identified through the literature review. The research method is described in Section 3. Section 4 presents a detailed analysis of the data through GTMA and provides the results which are discussed in Section 5. Conclusions are drawn in Section 6.

2. Background

2.1. Current status of industry 5.0 and related cybersecurity issues

Nowadays, it is important to adapt Industry 5.0 technology to cope with the competitive market. The target of Industry 5.0 is to create a human-centric, sustainable, and resilient base for industrial networked information, which is an open, smart art manufacturing platform [5,19]. Industry 5.0 paves the way for customized production systems and allows end-to-end value chain control throughout product life cycles more effectively and sustainably than has been historically possible [20,21]. Related technologies and capabilities include smart factories, cyber-physical systems, self-organization, more advanced distribution, procurement, product and service development systems, more effective adjustment to human demands, and increased sustainability and resource efficiency during the design of the industrial manufacturing process [22,20,23,24]. According to a 2014 report by PricewaterhouseCoopers, the European industry would invest €140 billion annually until 2020, with more than 80 percent of firms digitizing their value chains and having an 18 percent improvement in efficiency [25].The foundation of Industry 5.0 has nine major elements explained as follows:

Big Data and Analytics - Leverages increased computing power to gain insights from exceptionally massive and complex datasets [26,4].

Autonomous Robot – Automation designed to function collaboratively with humans and combine the benefits of automation, human creativity, and cognitive ability [20].

Simulation - Digitally mirroring physical systems to support decision-making with real-time analysis, minimizing downtime and quality failure [21,2].

Internet of Things (IoT) - Ubiquitous communication and data collection connectivity of electronic devices present in business operations [27].

Horizontal and Vertical System Integration - The technocentric integration and automation of internal business units, processes and technologies (vertical) and external value stream partners (horizontal) [21].

Cyber-Physical Systems (CPS) – Bi-dimensional systems characterized by the seamless integration of physical and digital technologies, enabling simultaneous self-optimization in both dimensions [28].

Cloud-based IT system – External digital storage and processing infrastructure that increases computing capability without investment in hardware purchase or maintenance [29,19].

Smart Additive manufacturing – Technologies that reduce manufacturing system footprints, lead times, and environmental impacts with the creation of digital inventories, mass customization and reduction of waste. Research and development portions of product lifecycles are also reduced through rapid prototyping [30,20,21].

Augmented reality – Real-time expansion of visual information through combined video and computer technologies to enhance training and decision-making in work environments [31,21].

To become and compete as an Industry 5.0 company, a company must adopt these nine technologies into a holistic socio-environmental strategy. As a result of the above discussion, we can conclude that Industry 5.0 offers a number of benefits and opportunities.

Cybersecurity is defined as the protection of IT hardware, software, and system-stored data from theft, damage, or hacking [32]. In the vast connectivity of Industry 5.0, cybersecurity is necessary to shield companies from losses resulting from cyber-attacks. Despite a decade of increased attention to cybersecurity expenditures, cyber-attacks continue to increase, costing an estimated $575 billion annually worldwide [33]. Many important types of industrial equipment can be easily hacked, causing damage to business systems [34]. From Cisco's

2018 Annual cybersecurity reports, 31 percent of organizations victimized by cyber-attacks experience damage to operational technology (OT), and 38 percent reported that attacks focused on information technology (IT) [34]. Additionally, 75 percent of experts recognize cybersecurity as a top priority, while only 16 percent of organizations are prepared to deal with cybersecurity challenges [34].

There are different types of cyber-physical attacks known within the industry as zero-day attacks, eavesdropping attacks, denial of service, false data injection attacks, and replay attacks [35]. These incursions may span the breadth of a network, requiring security solutions to match this connectivity from the manufacturing floor (OT) across all IT systems [35]. This is challenging because OT equipment generally does not contain the same computing power as IT. In such a challenging context, good security policies and techniques can help to minimize security breaches [35].

As the supply chains integrate with Industry 5.0, opportunities for cyber hackers and malicious suppliers to damage the supply chain are increasing. As a result, there is a demand for an effective cyber-threat detection system. Generally, security through obscurity is used, but it is insufficient. Actually, malicious suppliers can damage the system without understanding the system [36]. A 2015 survey report showed that because of Industry 5.0—which accounts for the Industry 5.0 technologies susceptible to attack—cyber-risk had increased from 36 percent to 48 percent and cited modular safeguards, decentralized architecture, and monitoring access as appropriate risk-reducers manufacturing firms should consider [37].

2.2. Study motivation and background

Since industry 5.0 works are not widely available in the literature, Industry 4.0 challenges were used as a baseline and expanded with the extant literature on Industry 5.0. To that end, relevant literature on Industry 4.0 is included. In the context of Industry 5.0, communications and cybersecurity cannot be viewed as separate processes. It is, therefore, essential for all manufacturers seeking Industry 5.0 benefits to understand the associated capabilities and risks. The cyber security-related challenges presented in this study may guide firms toward the development of such strategic initiatives. This subsection identifies published articles on cybersecurity, Industry 5.0, and the problem of cybersecurity within Industry 5.0 to better understand the challenges pertaining to industry 5.0 cybersecurity. It is noted that the progression from Industry 4.0 to Industry 5.0 may be viewed as an evolution of the technological 4.0 revolution to incorporate environmental and societal concerns for a more systematic approach ([38,39,2];). As cybersecurity relates largely to the 4.0 technologies, which are part of Industry 5.0, 4.0 research is included in the subsequent literature review and discussed under the moniker of Industry 5.0. Ilhan and Karaköse [40] suggested a simple and effective cybersecurity framework for repairing, updating, and renewing systems, generating a reference for Industry 5.0 cybersecurity requirements. On the other hand, Radanliev et al. [41] applied grounded theory to integrate five Industry 5.0 cyber trends, seven cyber risk frameworks, and two cyber risk models. They provided a deeper knowledge of a comprehensive economic effect assessment model for IoT cyber risk. In another study, Sarker and Furhad [42] offered a complete overview of AI-driven cybersecurity, which helped intelligent cybersecurity services and administration. In another study, Chhetri et al. [6] talked about the supply chain, product life cycle, and the many security problems that have accompanied enabling technologies in the Industry 5.0 era. In particular, the authors provided the latest research and trends in safeguarding the supply chain 5.0 and product life cycle, including key enabling technologies. Süzen [43] explained how cyber-attacks against Industry 5.0 occur, revealing the protection measures that end-users and businesses in the Industry 5.0 area should utilize against cyber threats. Pereira et al. [44] provided a framework for improving cybersecurity practices in Industry 5.0 through the identification of security challenges. In another research, Benias and Markopoulos [45] discussed the cybersecurity problems that specialists face in Industry 5.0. They provided real-life case studies as well as recommendations for successful cybersecurity. Sawik [33] provided a mixed-integer linear programming algorithm in the Industry 5.0 supply chain area for optimizing investment in cybersecurity. They utilized a recursive linearization approach for developing a sophisticated nonlinear stochastic combinatorial optimization model with a classical exponential function of breach probability turned into its linear equivalent. The resulting linear optimization model may be used to pick an optimal portfolio of security safeguards in order to reduce cybersecurity expenditure and the estimated losses from supply chain security breaches. Tuptuk and Hailes [8] examined the challenges faced by individuals desiring to safeguard smart manufacturing systems as the main elements of Industry 5.0. They also discussed different existing security systems, potential problems of systems, and cyber-attacks that may occur in the future. In line with this work, Culot et al. [46] described the importance of dynamic cybersecurity for Industry 5.0 with an outline of managerial challenges and innovative solutions.

Ervural and Ervural [9] analyzed the cybersecurity problems of Industry 5.0, such as IoT security dangers and vulnerabilities, industrial problems, the primary causes of cyber-attacks, the need for cybersecurity, and some cybersecurity strategies and approaches. In another study, Mukherjee et al. [47] aimed to enumerate all potential obstacles to Industry 5.0 adoption, rank them empirically and assess interdependencies at the organizational level. They used a multi-criteria decision-making methodology called the decision-making trial and evaluation laboratory method (DEMATEL) to detect obstacles and examine causal links. According to their findings, the most significant impediments were those related to expenses and financing systems, capacity flexibility, and training of human labor. They also provided a thorough overview of how the "Green, Resilient and Inclusive Development" (GRID) framework was implemented to find appropriate measures toward addressing the various detected obstacles. Karmaker et al. [48] identified Industry 5.0 implementation difficulties when dealing with the effects of SC disruptions brought on by the COVID-19 epidemic in an economy that was developing. They utilized the Best-Worst Method (BWM) and a combination of interpretive structural modelling (ISM) with cross-impact matrix multiplication applied to classification (MICMAC) analysis in their research. The authors concluded that senior managers must actively participate in the execution phase if Industry 5.0 attempts are to be successfully implemented to control the effect of COVID-19 on SC sustainability. In addition, Ghobakhloo et al. [49] created a strategic framework that explains how Industry 5.0 performs the functions meant to support sustainable growth. The authors built an Industry 5.0-enabled framework for sustainable growth using the interpretative structural modelling (ISM) technique to find the subsequent linkages between functions. According to the author's findings, Industry 5.0 promotes sustainable growth through 16 functions. In another work, Ali et al. [50] looked into what might have caused Bangladesh's banking sector's IT system to malfunction. The authors used a comprehensive analysis that combined flexible failure mode and effect analysis (FMEA) based on rough set theory and the technique for order of preference by similarity to ideal solution (TOPSIS) to assist the executives of the corresponding field in identifying and prioritizing the factors that led to the malfunction of the information technology (IT) systems in the banking industries. Their findings showed that the most important causes of the IT system's breakdown were cyber-attack, database hacking dangers, server collapse, connection disruption, erroneous broadcast data, and malware effects. To give a thorough overview of the subject, Corallo et al. [7] conducted a methodical literature review analyzing the way the current state of practice addresses cybersecurity awareness in the realm of IoT. Their comprehensive review served as a foundation for upcoming studies and developments in the area of cybersecurity awareness in environments related to the IoT model. Parker et al. [51] provided a summary of recent studies on supply chain, process management, and operational

cybersecurity challenges. They discussed adaptive control mechanisms, machine learning detection techniques, and encryption-decryption solutions for establishing safe communication. Table 1 represents the current themes within Industry 5.0 cybersecurity literature.

2.3. Research gap and contribution

The literature review reveals that several attempts have been conducted on Industry 5.0 cybersecurity challenges, but none applies any method to model the challenges sub challenges considering the interrelationships and inheritance among them and subsequently developing a comprehensive mathematical analysis to form an order. This study is being carried out to close this gap using graph theory and matrix approach (GTMA). The GTMA method is highly effective, especially when interdependencies between criteria and sub-criteria must be considered. GTMA is able to illustrate the interrelationship between the criteria and sub criteria of the alternatives [52]. Additionally, GTMA visualizes the criteria and sub-criteria and provides a hierarchical relationship structure between alternatives. Taking into account the inheritance and interdependence of the criteria when formulating the mathematical model, the GTMA is superior to other conventional approaches [53]. For instance, DEMATEL [54] and fuzzy cognitive maps (FCM) aim to construct a structural relationship instead of calculating weights [55]. By contrast, GTMA facilitates the evaluation of interdependencies among criteria and forms a hierarchy among them. To that end, in this study, GTMA approach play a significant role in assessing and ranking Industry 5.0 cybersecurity challenges by providing structured frameworks to model and analyze complex relationships and dependencies among various elements in the cybersecurity landscape Within this context, this study endeavors to achieve the following objectives: (i) assess Industry 5.0 cybersecurity challenges, (ii) rank the challenges using the GTMA, and (iii) provide countermeasures to surmount these challenges.

3. Research methodology

First, a study and analysis of extant literature was carried out to identify the cybersecurity challenges of Industry 5.0. Then GTMA approach was applied to model the challenges. Based on the inherent nature of the challenges and their interrelationship, GTMA defines the hierarchy of Industry 5.0 cybersecurity challenges. A study outline is shown in Fig. 1.

Phase 1: Identification of Industry 5.0 cybersecurity challenges

A thorough examination of peer-reviewed literature was conducted to identify Industry 5.0 cybersecurity challenges. To begin the analysis, Google Scholar and Scopus databases were queried using the following arbitrary keywords: *Industry 5.0 cybersecurity, Industry 5.0 cybersecurity vulnerability, Industry 5.0 cybersecurity problems, Industry 5.0 security, Industry 5.0 network security*, and *Industry 5.0 cybersecurity assessment*. This search conducted within the first six months of 2023 resulted in the aggregation of 125+ journal papers. This literature database was further screened, providing insight into the suitability and aptness of the subject matter as well as avoiding duplication and weak relevance to the topic. To narrow the candidate pool further, some publications were summarized to identify relevance to the following content: Industry 5.0 cybersecurity challenges; Industry 5.0 network security problems; Industry 5.0 implementation problems of cybersecurity. Following the implementation of these inclusion criteria, 30 journal papers were selected for further examination. The selected articles were reviewed based on the deductive approach, in which the key concept is to review the Industry 5.0 cybersecurity challenges and Industry 5.0 implementation problems through bibliometric analysis. This deductive approach employed coding and aggregation of key concepts, collapsing of similar groupings into conceptual distillations, and removal of unreinforced ideas. The review process used in this study is shown in the following Fig. 2.

Table 1
Current theme of Industry 4.0/5.0 Cybersecurity.

References	Approach	Application Area and Findings
Benias and Markopoulos [45]	Conceptual framework	Discussing Industry 5.0 cybersecurity and providing guidance for effective cybersecurity.
Pereira et al. [44]	Conceptual framework	Improving cybersecurity practice and identifying some security challenges of Industry 5.0.
Chhetri et al. [6]	Conceptual framework	Analyzing Industry 5.0 supply chain security and providing safeguarding strategies.
Ervural and Ervural [9]	Theoretical approach	Examining the cybersecurity challenges of Industry 5.0 and representing cybersecurity strategies.
Radanliev et al. [41]	Grounded theory	Integrating cyber risk models, frameworks, and Industry 5.0 trends to provide an assessment model for IoT cyber risk.
Tuptuk and Hailes [8]	Theoretical approach	Analyzing the challenges of smart manufacturing within Industry 5.0.
Culot et al. [46]	Theoretical approach	Summarizing the managerial challenges of cybersecurity, Industry 5.0, and recommended dynamic solutions.
Ilhan and Karaköse [40]	Conceptual framework	Providing repair, update, and renewal of Industry 5.0 cybersecurity systems and a simple and effective framework.
Süzen [43]	Conceptual framework	Examining the cyber-attacks of Industry 5.0 and offering protection measures.
Sawik [33]	A recursive linearization approach	Representing a mixed-integer linear programming algorithm in Industry 5.0 supply chain cybersecurity which helps to select an optimal portfolio of security safeguards.
Sarker and Furhad [42]	Artificial Intelligence (AI)	Providing a complete overview of AI-driven cybersecurity.
Mukherjee et al. [47]	Decision-making trial and evaluation laboratory method (DEMATEL)	Identifying obstacles to Industry 5.0 adoption and revealing expenses and financing systems as a main cause.
Karmaker et al. [48]	Best-Worst Method (BWM) and a combination of structural modeling (ISM) with cross-impact matrix multiplication applied to classification (MICMAC)	Analyzing Industry 5.0 supply chain disruption and suggesting senior management active participation as mitigation.
Ghobakhloo et al. [49]	Interpretative Structural modeling (ISM) technique	Industry 5.0 promotes sustainable growth through 16 functions.
Ali et al. [50]	A combination of Failure Mode and Effect Analysis (FMEA) and Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS)	Suggesting banking IT systems cyber-attacks and database hacking are the main causes of cyber-disruption.
Corallo et al. [7]	A methodical literature review	Analyzing the way in which the current state of the practice addresses cybersecurity awareness in the realm of IoT.
Parker et al. [51]	Adaptive control mechanisms, machine learning, and encryption-decryption solutions	Focusing on supply chain, process management, and operational cybersecurity challenges and providing solutions for establishing safe communication.

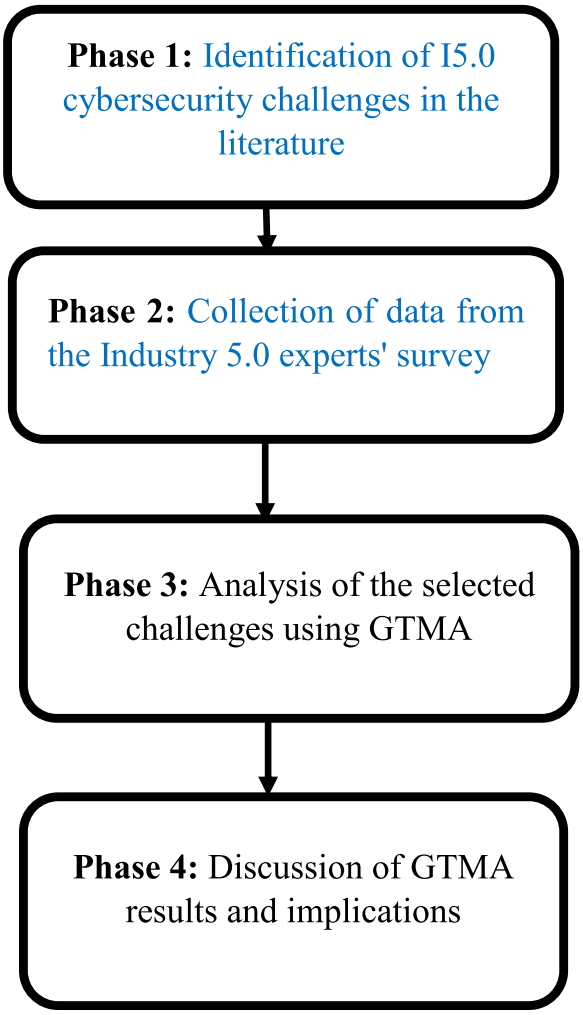


Fig. 1. Research Methodology.

Critical cybersecurity challenges are recognized after studying literature and consulting with experts. The 10 main challenges and 30 sub-challenges are shown in Table 2.

3.1. Overview of challenges and sub-challenges

Whatever the cause, firms have experienced difficulty locating and training cybersecurity professionals with the necessary aptitude to excel in the modern environment [46,56]. This reality is expressed here as the *absence of skilled employees and training (ASET)* challenge. Associated sub-challenges are lack of qualified specialists [57], employees' trouble with new skills [58], and insufficient training [59]. Beyond the workforce, firms have also suffered from poor cybersecurity owing to inadequate funding. *Insufficient strategy to fund cybersecurity (ISFCS)* is driven by a general failure by management to prioritize cybersecurity [46,60]. The next identified challenge is the result of ambiguous role definitions within large systems. As systems increase in interdependent scope, roles and responsibilities are being inadequately characterized and delineated, resulting in *poorly defined accountability of cybersecurity (PDACSC)* [61,57]. Associated sub-challenges include inadequately planned procurement contracts [56], lacking liability-related law [58], and an ever-expanding variety of stakeholders [57]. In addition to accountability, there is insufficient homogeneity across the many Industry 5.0 cybersecurity stakeholders. The associated challenge is identified as *unstandardized Industry 5.0 security policies (UISPC)* [44,8]. Sub-challenges include different policies in branches of large manufacturing organizations [62], lack of systemic way [57], and lack of security standards research [56]. The expansion of supply chains inherently creates weak points as resources are stretched to cover new scopes. In this research, this is described as the *supply chain vulnerabilities (SCV)* challenge [6,63,64]. The contributing sub-challenges are a more independent supply chain [65], different degrees of cybersecurity in the supply chain [66], and lack of proper scaling when considering supplier cybersecurity [25]. Another challenge described as *deficiency in interoperability and common communication language (DICCL)* centers on the intersection of operations and automation and covers the difficulties arising from not only the integration of disparate technologies but also layering novel onto heritage technologies that are compounded by expansive networks [67,68]. Sub-challenges for DICCL include difficult

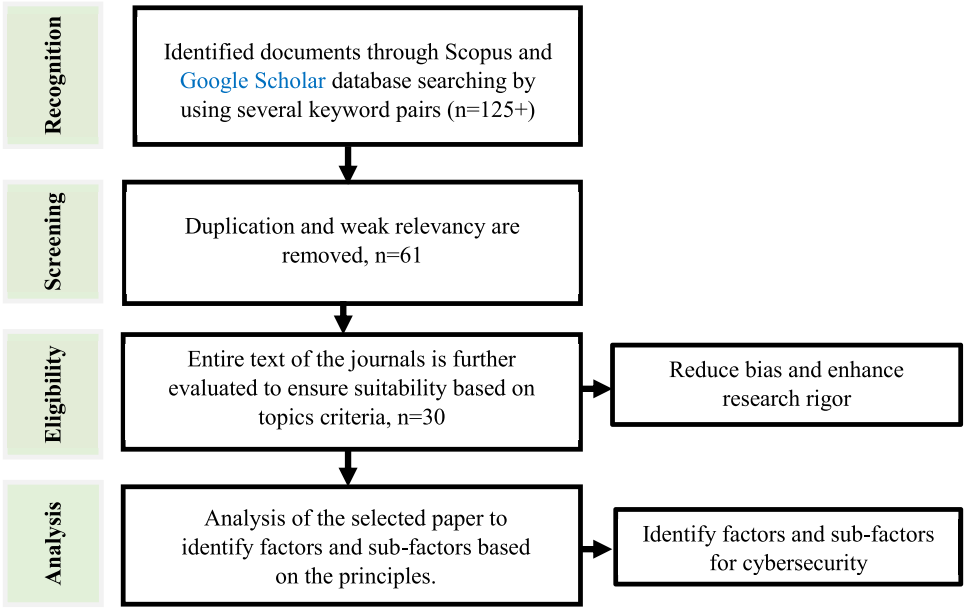


Fig. 2. Flow Diagram of the Factor and Sub-Factor Extraction Process.

Table 2
Cybersecurity Challenges of Industry 5.0 and Their Sub-Challenges.

	Challenge	Code		Sub Challenge
1	**Absence of skilled employees and training**	ASET		
			1.1	Lack of qualified specialists
			1.2	Employees' trouble with new skills
			1.3	Insufficient training
2	**Insufficient strategy to fund cybersecurity**	ISFCS		
			2.1	Cybersecurity is not recognized as a high-level management issue
			2.2	Cybersecurity generates profit, not directly
			2.3	Keeping stability between cost and the need for security
3	**Poorly defined accountability of cybersecurity**	PDACSC		
			3.1	Procurement contracts have less planning
			3.2	Lacking liability-related law
			3.3	Huge variety of stakeholder
4	**Unstandardized Industry 5.0 security policies**	UISPC		
			4.1	Different policies in branches of large manufacturing organizations
			4.2	Lack of systemic way
			4.3	Lack of security standards research
5	**Supply chain vulnerabilities**	SCV		
			5.1	More interdependent supply chain
			5.2	Different degrees of cybersecurity in the supply chain
			5.3	Lack of proper scaling when considering supplier cybersecurity
6	**Deficiency in interoperability and common communication language**	DICCL		
			6.1	Tough to Secure integration of several devices
			6.2	Hard to ensure a common baseline of security among devices, platforms, and frameworks
			6.3	Interconnectivity between Industry 5.0 devices and legacy systems is challenging
7	**Embedded technical constraints**	ETC		
			7.1	No proper monitoring system
			7.2	Few consider advanced encryption or authentication
			7.3	Old devices and techniques are less ideal for cybersecurity
8	**Insufficient government patronization**	IGP		
			8.1	Lack of law to ensure cybersecurity
			8.2	Insufficient funding for research and development projects
			8.3	Lack of response to a hacking incident
9	**Non-availability of cybersecurity curriculum in education**	NACSCE		
			9.1	Inadequate collaboration between industry and university
			9.2	Absence of planning commission to reshape curriculum
			9.3	Cybersecurity course is not compulsory
10	**Emergent cybersecurity trends**	ECST		
			10.1	Growing cyberattack
			10.2	Lack of proper cybersecurity updates
			10.3	Flexibility of cybersecurity structure

to secure integration of several devices [69], hard in ensuring a common baseline of security among devices, platforms, and frameworks [46], and interconnectivity between Industry 5.0 devices and legacy system is challenging [70]. Not all the challenges are systems-related, however. Some challenges, such as *embedded technical constraints (ETC)* describe a list of discrete unsolved technical problems [57,71]. ETC sub-challenges include no proper monitoring system [72], few consider advanced encryption [57], and old devices and techniques are less ideal for cybersecurity [25]. Governmental involvement is also identified as a challenge to the advancement of effective cybersecurity. Titled *insufficient government patronization (IGP)*, this challenge includes sub-challenges of lack of law to ensure cybersecurity [73], insufficient funding of research and development projects, and lack of response to a hacking incident [74]. The next challenge arises from insufficient or non-existent cybersecurity programs within the education system. *Non-availability of cybersecurity curriculum in education (NACSCE)* is a direct contributor to ASET as well as other challenges plaguing the overall quality of Industry 5.0-wide cybersecurity. Sub challenges such as inadequate collaboration between industry and university [75], absence of planning commission to reshape the curriculum [76], and cybersecurity course is not compulsory [77] frame the level and seriousness of the deficiency in education. The final challenge addresses the stochastic nature of the problem in *emergent cybersecurity trends (ECST)* [78,79]. Supporting sub-challenges are growing cyber-attacks [34], lack of proper cybersecurity updates [9], and flexibility of cybersecurity structure [8], which characterize a theme of urgency to build resilient systems capable of quickly adapting to unconventional disruptions.

The experts' profiles are shown in Table 3. In the final analysis stage of screening, select papers were scrutinized using root cause analysis to understand the challenges at a fundamental level. This created a natural distillation of concepts from real-world instances to underlying drivers of cybersecurity failure.

Phase 2: Accumulation of data from experts

Table 3
Experts' Backgrounds.

Expert	Job title	Years of experience
1	Executive officer of data security	5
2	Manager	7
3	Manager	10
4	Director	12

In this study, a two-stage data-collection survey is conducted. At first, the challenges are identified based on a literature review and expert opinion. In the second stage, necessary data is collected from I5.0 experts to model the challenges through GTMA. Specialists or responders with a high level of expertise and insight into the Industry 5.0 cybersecurity topic were chosen as the participants able to make a significant contribution to this study. Email invitations were given to the 10 potential participants. Four out of 10 participants agreed to participate. Past research has shown that robust analysis is possible from a four-to-10-participant survey dataset [80]. Expert opinions were gathered through a series of round-table interviews, email exchanges, and telephone conversations. Table 3 shows the experts' profiles as well as their years of relevant experience.

Phase 3: Analysis of selected challenges using GTMA

In this phase, GTMA is applied to evaluate the identified challenges of industry 5.0 cybersecurity and determine their relative importance. GTMA is explained in Section 4.1, followed by an explanation of the research dataset and analysis in Section 4.2. Sections 4.3 through 4.5 detail the application of GTMA analysis.

Phase 4: Discussion of GTMA results and implications

In this phase, the resultant hierarchy is presented along with a detailed discussion of the analysis results. The academic and industrial implications of prioritizing Industry 5.0 cybersecurity challenges are given to conclude with recommendations for both sectors.

4. Data analysis

4.1. Proposed technique

GTMA was selected as the analytical approach, having proven effective in a variety of applications, including vendor and production process selection and supply chain management [55]. Other methods such as flow diagrams, representation vis-à-vis blocks, schematic representations, etc., which illustrate the correlation between variables, have also been applied. GTMA, in contrast, combines graphical and mathematical analysis and incorporates the effects of variable interdependency.

To illustrate the effectiveness of GTMA at a high level, a generic manufacturing example is given: managers, when setting up a new production line, may choose from an array of acceptable manufacturing methods. Each alternative will have different impacts on the associated product factors of quality, cost, technical capability, and producibility. Trades are likely needed between quality and cost. GTMA can be used to select the best manufacturing method for the new production line taking into consideration both the relative importance of each variable and the interdependence amongst them. Interdependence is a key tenant of systems thinking, which plays a vital role in the successful navigation of complexity contained within Industry 5.0 manufacturing systems [53].

Within GTMA, the matrix approach investigates the digraph model and gives a mathematical value known as a matrix permanent describing the system or problem [81,82]. Graph theory is combined with combinatorial mathematics and matrix algebra, resulting in both graphical and numerical models describing the system in question [18]. Interested readers are directed to Gandhi et al. [83] and Gandhi & Agrawal [84] for a full detailed explanation of GTMA. Here, GTMA is a suitable model because of the need to consider interrelationships and give weight to the problem challenges. The analysis follows four steps:

I. First, identify the cybersecurity of Industry 5.0 related challenges explained in Section 3.
II. Second, construct digraphs of each challenge based on identified interrelationships. This is the portion of the approach borrowed from graph theory. Fig. 3 displays a sample digraph containing nodes SCV_i and directed edges f_{ij}. Each node represents a sub-challenge—in this case, the sub-challenges associated with Supply Chain Vulnerabilities—while each directed edge represents the interrelationship between sub-challenges. The influence, for example, of challenge SCV_1 on SCV_2 is represented by directed edge f_{12}. Significance values f_{ij} are assigned from Expert input to directed edges using the scale in Table 6. In the event challenge j is described as more significant than challenge i, the significance value is expressed as f_{ji} [85].
III. Third, digraphs are converted into matrices. Each matrix is called a variable permanent matrix (VPM) generalized in Fig. 4. This is an $N \times N$ matrix where N is the number of challenges. The diagonal elements f_i represent the importance of each sub challenge relative to the main challenge and the off-diagonal elements f_{ij} represent the importance of the i^{th} challenge over the j^{th} challenge [55].

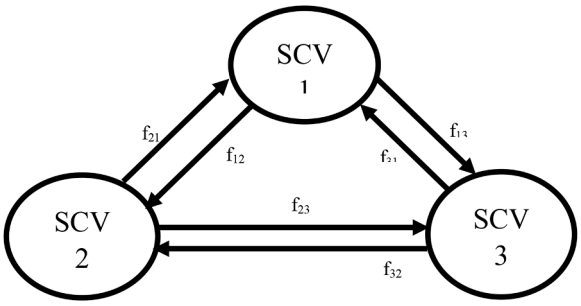


Fig. 3. Sample Digraph.

The matrix values are obtained from experts using the survey (see appendix B) and the scales in Table 4 [53] and Table 5 [55] .

I. Fourth, permanent values are calculated from each VPM, and the resultant values are ordered to reveal priority. The permanent is chosen over the determinant for its incorporation of all information stored in the VPM. The determinant, in contrast, removes some information through the negative signs in the calculation. Just as digraphs are constructed for each sub-challenge, one is also created for the set of 10 main Industry 5.0 cybersecurity challenges as follows: CH1: absence of skilled employee training (ASET); CH2: insufficient strategy to fund cybersecurity (ISFCS); CH3: poorly defined accountability of cybersecurity (PDACS); CH4: unstandardized Industry 5.0 security policies (UISP); CH5: supply chain vulnerabilities (SCV); CH6: deficiency in interoperability and common communication language (DICCL); CH7: embedded technical constraints (ETC); CH8: insufficient government patronization (IGP); CH9: non-availability of cybersecurity curriculum in education (NACSCE);

	sch1	sch2	sch3
sch1	f_1	f_{12}	f_{13}
sch2	f_{21}	f_2	f_{23}
sch3	f_{31}	f_{32}	f_3

Fig. 4. Variable Permanent Matrix.

Table 4
The Scale of Impact of Sub-Challenges [53].

scale of importance	rating (f_i)
Extremely low	1
Low	2
Below average	3
Average	4
Above average	5
High	6
Extremely high	7

Table 5
Relative Significance of Sub-Challenges [55].

description	relative significance of challenges	
	f_{xy}	$f_{yx} = 10 - f_{xy}$
Comparing challenges are equally significance	5	5
One challenge is moderately important over another	6	4
One challenge is strongly important over another	7	3
One challenge is very strongly important over another	8	2
One challenge is extremely important over another	9	1
One challenge is extraordinarily important over another	10	0

CH10: Emergent cybersecurity trends (DFECST). This digraph is displayed in Fig. 5.

As digraph edges and nodes increase in number, so does the digraph increase in visual complexity. Rather than rendering it useless, this trait drives the need for the transformation of the information into matrix forms. Such a Matrix [M] is shown in Fig. 6 as an $N \times N$ matrix where N is the number of main challenges. The diagonal elements E_i represent the importance of each main challenge (based on sub-challenge VPM permanent values), while the off-diagonal elements f_ij where i≠j represent the relative importance of each challenge to each other challenge. More specifically, this is the importance of the ith challenge over the jth challenge.

$$[M] = \begin{array}{c} \\ CH1 \\ CH2 \\ CH3 \\ CH4 \\ CH5 \\ CH6 \\ CH7 \\ CH8 \\ CH9 \\ CH10 \end{array} \begin{array}{c} \begin{array}{cccccccccc} CH1 & CH2 & CH3 & CH4 & CH5 & CH6 & CH7 & CH8 & CH9 & CH10 \end{array} \\ \begin{bmatrix} E_1 & f_{12} & f_{13} & f_{14} & f_{15} & f_{16} & f_{17} & f_{18} & f_{19} & f_{110} \\ f_{21} & E_2 & f_{23} & f_{24} & f_{25} & f_{26} & f_{27} & f_{28} & f_{29} & f_{210} \\ f_{31} & f_{32} & E_3 & f_{34} & f_{35} & f_{36} & f_{37} & f_{38} & f_{39} & f_{310} \\ f_{41} & f_{42} & f_{43} & E_4 & f_{45} & f_{46} & f_{47} & f_{48} & f_{49} & f_{410} \\ f_{51} & f_{52} & f_{53} & f_{54} & E_5 & f_{56} & f_{57} & f_{58} & f_{59} & f_{510} \\ f_{61} & f_{62} & f_{63} & f_{64} & f_{65} & E_6 & f_{67} & f_{68} & f_{69} & f_{610} \\ f_{71} & f_{72} & f_{73} & f_{74} & f_{75} & f_{76} & E_7 & f_{78} & f_{79} & f_{710} \\ f_{81} & f_{82} & f_{83} & f_{84} & f_{85} & f_{86} & f_{87} & E_8 & f_{89} & f_{810} \\ f_{91} & f_{92} & f_{93} & f_{94} & f_{95} & f_{96} & f_{97} & f_{98} & E_9 & f_{910} \\ f_{101} & f_{102} & f_{103} & f_{104} & f_{105} & f_{106} & f_{107} & f_{108} & f_{109} & E_{10} \end{bmatrix} \end{array}$$

In another study, Forbert and Marx [86] proposed a common formula for permanent function of $N \times N$ matrix [M] which is described in Equation in 1.

$$per(M) = \sum_{p} \prod_{i=1}^{N} r_i P(i) \tag{1}$$

Here, the sum is the total amount of permutations P. For calculating the permanent function, a program in Matlab is used. This code shall be made available upon request.

4.2. Resources

Cybersecurity is a vital component of Industry 5.0. Industry 5.0 is built on Industry 4.0 and aims to address its shortcomings, such as placing less emphasis on social justice and sustainability [2]. For this study, the opinion of four experts from different German Industry 5.0 companies were utilized for investigation. Their backgrounds are shown in Table 3. The research team consulted with these experts and collected the necessary data using a bespoke survey tool (Appendix B).

4.3. Building the digraph

In this section, the interrelationships among the sub-challenges of the main challenges of Industry 5.0 cybersecurity are examined and shown in terms of diagraphs in Figs. 7-16.

The digraph of insufficient strategy to fund cybersecurity (ISFCS) challenge is displayed in Fig. 8.

Fig. 9 illustrates the relationships between the sub-challenges of the poorly defined accountability of cybersecurity (PDACS) challenge.

Fig. 10 represents the interrelationships between the sub-challenges of the unstandardized Industry 5.0 security policies (UISP) challenge.

The digraph of supply chain vulnerabilities (SCV) challenge is displayed in Fig. 11.

Interrelationship among the sub-challenges of deficiency in interoperability and common communication language (DICCL) challenge is presented in Fig. 12.

Fig. 13 represents the interrelationships between the sub-challenges of the embedded technical constraints (ETC) challenge.

Fig. 14 illustrates the relationships between the sub-challenges of insufficient government patronization (IGP) challenge.

Interrelationship among the sub-challenges of the non-availability of cybersecurity curriculum in education (NACSCE) challenge is shown in Fig. 15.

Fig. 16 shows the relationships between the sub-challenges of emerging cybersecurity trends (ECST) challenges.

4.4. Development of matrix and calculation of permanent

The digraphs of each industry 5.0 challenge above are converted into matrix form and shown as VPMs as follows:

$$\text{Permanent (ASET)} = \begin{bmatrix} ASET1 & \text{f12} & \text{f13} \\ \text{f21} & ASET2 & \text{f23} \\ \text{f31} & \text{f32} & ASET3 \end{bmatrix}$$

$$\text{Permanent (ISFCS)} = \begin{bmatrix} ISFCS1 & \text{f12} & \text{f13} \\ \text{f21} & ISFCS2 & \text{f23} \\ \text{f31} & \text{f32} & ISFCS3 \end{bmatrix}$$

$$\text{Permanent (PDACS)} = \begin{bmatrix} PDACS1 & \text{f12} & \text{f13} \\ \text{f21} & PDACS2 & \text{f23} \\ \text{f31} & \text{f32} & PDACS3 \end{bmatrix}$$

$$\text{Permanent (UISP)} = \begin{bmatrix} UISP1 & \text{f12} & \text{f13} \\ \text{f21} & UISP2 & \text{f23} \\ \text{f31} & \text{f32} & UISP3 \end{bmatrix}$$

$$\text{Permanent (SCV)} = \begin{bmatrix} SCV1 & \text{f12} & \text{f13} \\ \text{f21} & SCV2 & \text{f23} \\ \text{f31} & \text{f32} & SCV3 \end{bmatrix}$$

$$\text{Permanent (DICCL)} = \begin{bmatrix} DICCL1 & \text{f12} & \text{f13} \\ \text{f21} & DICCL2 & \text{f23} \\ \text{f31} & \text{f32} & DICCL3 \end{bmatrix}$$

$$\text{Permanent (ETC)} = \begin{bmatrix} ETC1 & \text{f12} & \text{f13} \\ \text{f21} & ETC2 & \text{f23} \\ \text{f31} & \text{f32} & ETC3 \end{bmatrix}$$

$$Permanent(IGP) = \begin{bmatrix} IGP1 & f12 & f13 \\ f21 & IGP2 & f23 \\ f31 & f32 & IGP3 \end{bmatrix}$$

$$\text{Permanent (NACSCE)} = \begin{bmatrix} NACSCE1 & \text{f12} & \text{f13} \\ \text{f21} & NACSCE2 & \text{f23} \\ \text{f31} & \text{f32} & NACSCE3 \end{bmatrix}$$

$$\text{Permanent (ECST)} = \begin{bmatrix} DFECST1 & \text{f12} & \text{f13} \\ \text{f21} & DFECST2 & \text{f23} \\ \text{f31} & \text{f32} & DFECST3 \end{bmatrix}$$

After establishing VPMs, permanent values are calculated for each

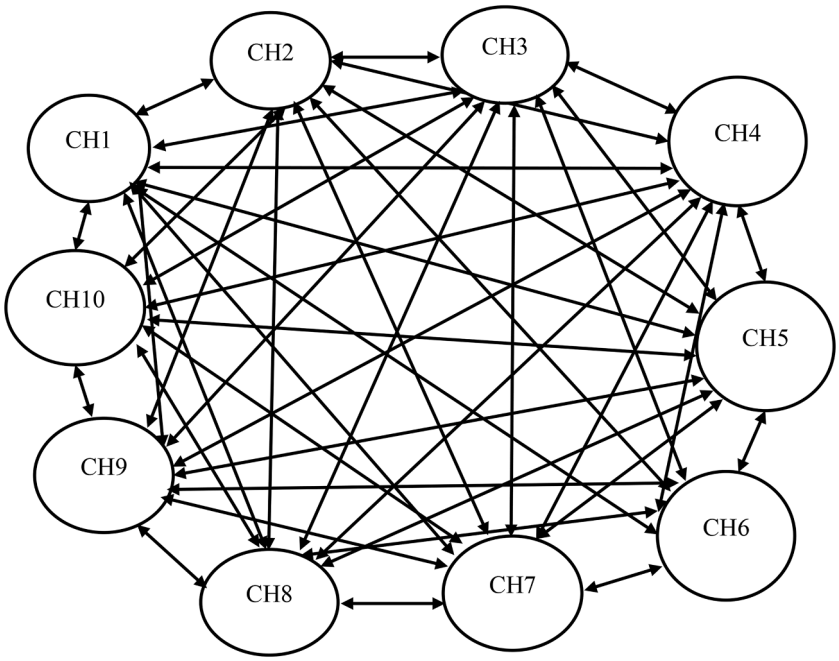


Fig. 5. Digraph of Main Industry 5.0 Cybersecurity Challenges.

$$[M] = \begin{array}{c} \\ CH1 \\ CH2 \\ CH3 \\ CH4 \\ CH5 \\ CH6 \\ CH7 \\ CH8 \\ CH9 \\ CH10 \end{array} \begin{array}{c} \begin{array}{cccccccccc} CH1 & CH2 & CH3 & CH4 & CH5 & CH6 & CH7 & CH8 & CH9 & CH10 \end{array} \\ \begin{bmatrix} E_1 & f_{12} & f_{13} & f_{14} & f_{15} & f_{16} & f_{17} & f_{18} & f_{19} & f_{110} \\ f_{21} & E_2 & f_{23} & f_{24} & f_{25} & f_{26} & f_{27} & f_{28} & f_{29} & f_{210} \\ f_{31} & f_{32} & E_3 & f_{34} & f_{35} & f_{36} & f_{37} & f_{38} & f_{39} & f_{310} \\ f_{41} & f_{42} & f_{43} & E_4 & f_{45} & f_{46} & f_{47} & f_{48} & f_{49} & f_{410} \\ f_{51} & f_{52} & f_{53} & f_{54} & E_5 & f_{56} & f_{57} & f_{58} & f_{59} & f_{510} \\ f_{61} & f_{62} & f_{63} & f_{64} & f_{65} & E_6 & f_{67} & f_{68} & f_{69} & f_{610} \\ f_{71} & f_{72} & f_{73} & f_{74} & f_{75} & f_{76} & E_7 & f_{78} & f_{79} & f_{710} \\ f_{81} & f_{82} & f_{83} & f_{84} & f_{85} & f_{86} & f_{87} & E_8 & f_{89} & f_{810} \\ f_{91} & f_{92} & f_{93} & f_{94} & f_{95} & f_{96} & f_{97} & f_{98} & E_9 & f_{910} \\ f_{101} & f_{102} & f_{103} & f_{104} & f_{105} & f_{106} & f_{107} & f_{108} & f_{109} & E_{10} \end{bmatrix} \end{array}$$

Fig. 6. Matrix [*M*].

sub-challenge and each expert, respectively (interested readers are directed to Appendix C for a more detailed list). These values are displayed in Table 6. The permanent values for *absence of skilled employees and training* based on expert data are shown below.

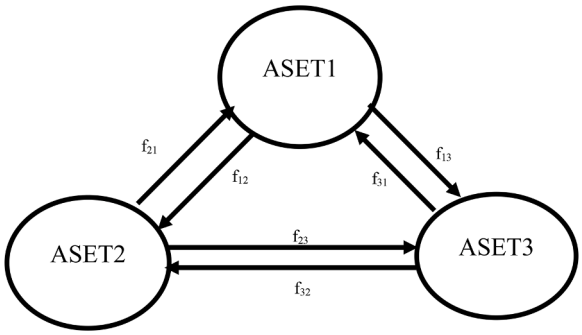


Fig. 7. Digraph of Absence of Skilled Employees and Training (ASET).

$$Permanent^{Expert1}(ASET) = \begin{bmatrix} 4 & 5 & 6 \\ 5 & 3 & 6 \\ 4 & 4 & 2 \end{bmatrix} = 482$$

$$Permanent^{Expert2}(ASET) = \begin{bmatrix} 3 & 4 & 8 \\ 6 & 4 & 7 \\ 2 & 3 & 2 \end{bmatrix} = 399$$

$$Permanent^{Expert3}(ASET) = \begin{bmatrix} 4 & 6 & 2 \\ 4 & 2 & 5 \\ 8 & 5 & 3 \end{bmatrix} = 508$$

$$Permanent^{Expert4}(ASET) = \begin{bmatrix} 4 & 6 & 8 \\ 4 & 2 & 4 \\ 2 & 6 & 3 \end{bmatrix} = 464$$

4.5. Mean permanent values

To maintain the specificity of each expert's responses, mean VPM

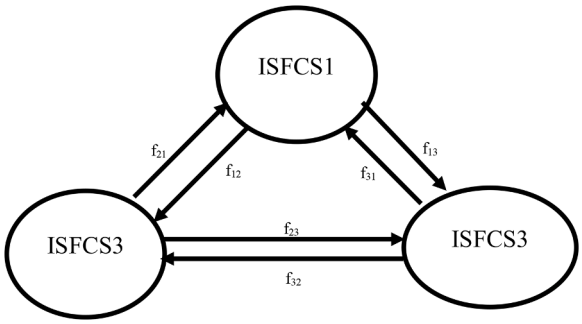


Fig. 8. Digraph of Insufficient Strategy to Fund Cybersecurity (ISFCS).

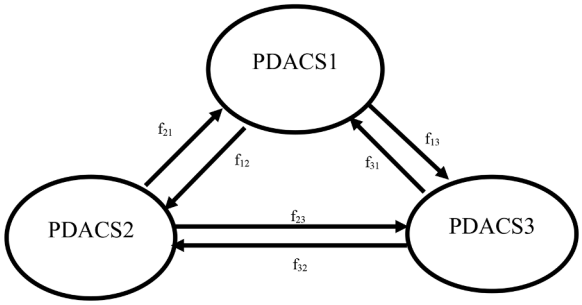


Fig. 9. Digraph of Poorly Defined Accountability of Cybersecurity (PDACS).

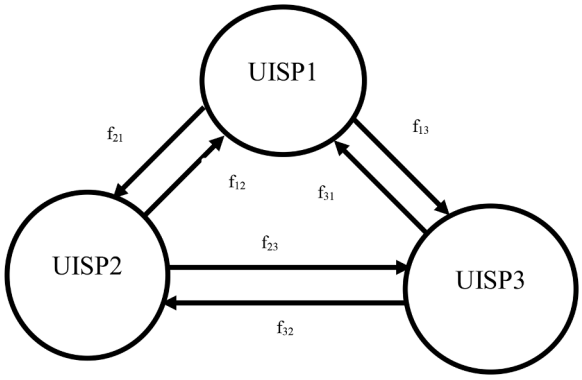


Fig. 10. Digraph of Unstandardized Industry 5.0 Security Policies (UISP).

values were calculated using all the original survey response data. An overview of this calculation is shown below, followed by the calculations for each expert mean sub-challenge permanent $permanent_{\mu}(sub-challenge)$.

$$VPM_{\mu}(ASET) = \begin{bmatrix} 4 & 5 & 6 \\ 5 & 3 & 6 \\ 4 & 4 & 2 \end{bmatrix} + \begin{bmatrix} 3 & 4 & 8 \\ 6 & 4 & 7 \\ 2 & 3 & 2 \end{bmatrix} + \begin{bmatrix} 4 & 6 & 2 \\ 4 & 2 & 5 \\ 8 & 5 & 3 \end{bmatrix} + \begin{bmatrix} 4 & 6 & 8 \\ 4 & 2 & 4 \\ 2 & 6 & 3 \end{bmatrix}$$

$$= \frac{\begin{bmatrix} 15 & 21 & 24 \\ 19 & 11 & 22 \\ 16 & 18 & 10 \end{bmatrix}}{4}$$

$$= \begin{bmatrix} 3.75 & 5.25 & 6.0 \\ 4.75 & 2.75 & 5.50 \\ 5.00 & 4.50 & 2.50 \end{bmatrix}$$

$$permanent_{\mu}(ASET) = 490.69$$

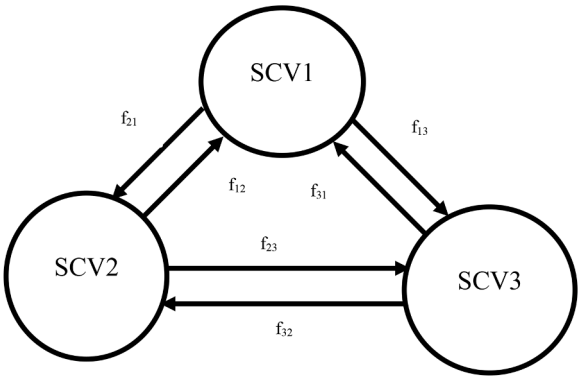


Fig. 11. Digraph of Supply Chain Vulnerabilities (SCV).

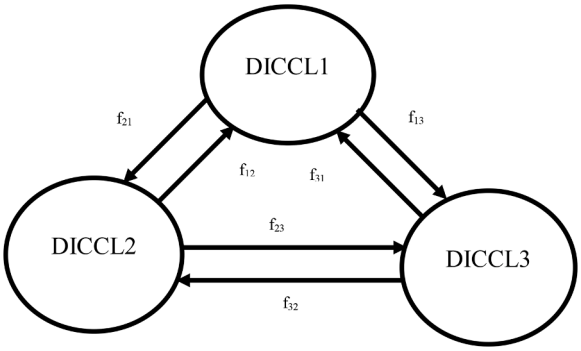


Fig. 12. Digraph of Deficiency in Interoperability and Common Communication Language (DICCL).

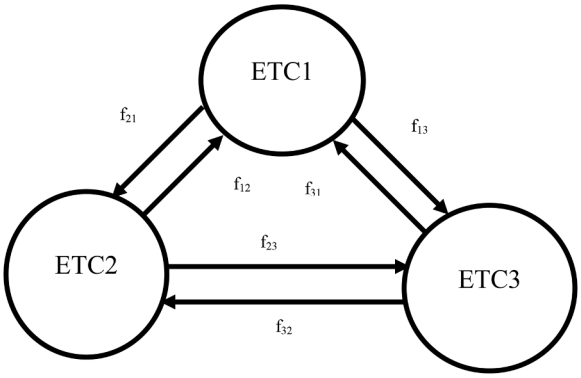


Fig. 13. Digraph of Embedded Technical Constraints (ETC).

The same procedure is carried out for each sub-challenge. The results are provided below. A summary table of these results is shown in Table 8.

$$permanent_{\mu}(ISFCS) = \begin{bmatrix} 2.50 & 3.75 & 3.5 \\ 6.25 & 2.75 & 3.75 \\ 6.50 & 6.25 & 1.50 \end{bmatrix} = 394.75$$

$$permanent_{\mu}(PDACS) = \begin{bmatrix} 2.00 & 5.25 & 5.00 \\ 4.75 & 1.25 & 5.75 \\ 5.00 & 4.25 & 1.25 \end{bmatrix} = 366.30$$

$$permanent_{\mu}(UISP) = \begin{bmatrix} 2.25 & 7.50 & 4.50 \\ 2.50 & 2.75 & 5.75 \\ 5.50 & 4.25 & 2.25 \end{bmatrix} = 464.16$$

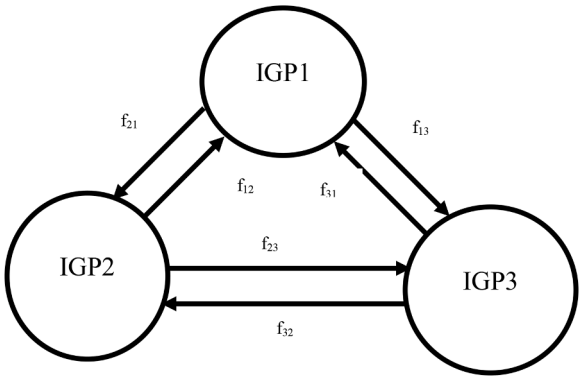


Fig. 14. Digraph of Insufficient Government Patronization (IGP).

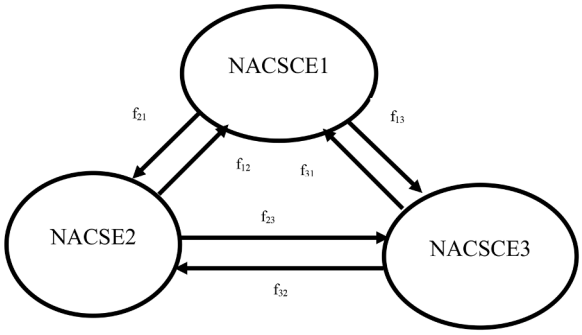


Fig. 15. Digraph of Non-Availability of Cybersecurity Curriculum in Education (NACSCE).

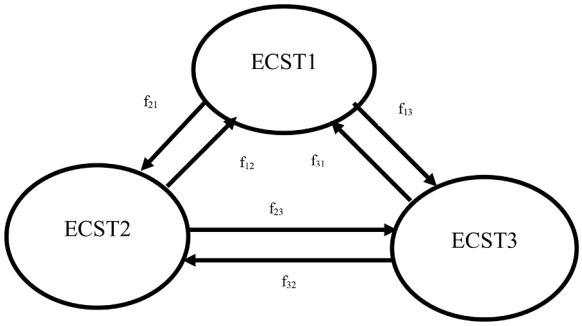


Fig. 16. Digraph of Emerging Cybersecurity Trends (ECST).

$$permanent_{\mu}(SCV) = \begin{bmatrix} 5.00 & 5.25 & 5.50 \\ 4.75 & 3.00 & 5.50 \\ 4.50 & 4.50 & 3.25 \end{bmatrix} = 575.30$$

$$permanent_{\mu}(DICCL) = \begin{bmatrix} 3.00 & 7.00 & 5.25 \\ 3.00 & 2.50 & 3.50 \\ 4.75 & 6.50 & 2.25 \end{bmatrix} = 413.47$$

$$permanent_{\mu}(ETC) = \begin{bmatrix} 2.25 & 6.25 & 4.75 \\ 3.75 & 2.50 & 5.00 \\ 5.25 & 6.00 & 4.75 \end{bmatrix} = 492.52$$

$$permanent_{\mu}(IGP) = \begin{bmatrix} 2.00 & 5.25 & 6.00 \\ 4.75 & 2.50 & 5.75 \\ 5.00 & 4.25 & 3.00 \end{bmatrix} = 440.56$$

Table 6
The Permanent Values of VPMs for Each Challenge by Expert.

Challenge	Expert 1	Expert 2	Expert 3	Expert 4
ASET	482	399	508	464
ISFCS	375	348	408	411
PDACS	350	352	366	390
UISP	474	442	504	441
SCV	533	553	577	607
DICCL	378	377	432	434
ETC	478	439	490	475
IGP	465	392	435	422
NACSCE	504	446	528	497
ECST	503	481	490	501

$$permanent_{\mu}(NACSCE) = \begin{bmatrix} 4.25 & 8.00 & 6.25 \\ 2.00 & 3.00 & 5.00 \\ 3.75 & 5.00 & 5.50 \end{bmatrix} = 547.19$$

$$permanent_{\mu}(ECST) = \begin{bmatrix} 3.75 & 6.5 & 5.25 \\ 3.50 & 3.00 & 6.25 \\ 4.75 & 3.75 & 4.25 \end{bmatrix} = 569.08$$

4.6. Results

GTMA analysis results in the form of Industry 5.0 cybersecurity challenge prioritization are shown below for each expert. A summary of the results is given in Table 7. Similarities are noted among the results for each expert. Examples include the clear priority of supply chain vulnerabilities and the non-availability of cybersecurity curriculum in education. Further similarities exist and generally cross-validate the results.

Priority order for Expert 1:

SCV> NACSCE> ECST> ASET> ETC> UISP> IGP> DICCL> ISFCS> PDACS

Priority order for Expert 2:

SCV> ECST> NACSCE> UISP> ETC> ASET> IGP> DICCL> PDACS> ISFCS

Priority order for Expert 3:

SCV> NACSCE> ASET> UISP> ECST > ETC> IGP> DICCL> ISFCS > PDACS

Priority order for Expert 4:

SCV> ECST> NACSCE> ETC> ASET> UISP> DICCL> IGP> ISFCS> PDACS

The overall prioritization considering all expert data, is calculated using the mean VPMs. The greater the permanent value, the higher the priority of the challenge. The resulting overall ranking of the challenges is shown in Fig. 17.

5. Discussion

5.1. Discussion of results

This section includes a challenge-wise discussion of the findings. Matrix permanent values are given, followed by a brief presentation of supporting ideas that validate the results.

Supply chain vulnerabilities: The permanent value of the *supply chain vulnerabilities* for experts 1, 2, 3, and 4 are 533, 553, 577, and 570, respectively. The permanent value of supply chain vulnerabilities is highest for every expert. Industry 5.0 increases the efficiency of the supply chain, but supply chain networks have inherent security flaws that hackers are able to exploit [65]. The increasing system complexity generated by horizontally integrated value chains expands the disruptive potential of cyber-attacks. Effective solutions that will secure the integrated IoT of Industry 5.0 require coordinated cooperation by key personal across these value chains [57]. Third-party risk ratings are recommended to audit suppliers on a regular basis [46].

Table 7
Ranking of cybersecurity challenges of Industry 5.0 for every Expert.

Challenge	Expert 1	rank	Expert 2	rank	Expert 3	rank	Expert 4	rank
ASET	482	4	399	6	508	3	464	5
ISFCS	375	9	348	10	408	9	411	9
PDACS	350	10	352	9	366	10	390	10
UISP	474	6	442	4	504	4	441	6
SCV	533	1	553	1	577	1	607	1
DICCL	378	8	377	8	432	8	434	7
ETC	478	5	439	5	490	6	475	4
IGP	465	7	392	7	435	7	422	8
NACSCE	504	2	446	3	528	2	497	3
ECST	503	3	481	2	490	5	501	2

Table 8
Overall ranking of the cybersecurity challenges of Industry 5.0.

challenges	index value	ranking
SCV	575.30	1
ECST	569.08	2
NACSCE	547.19	3
ETC	492.52	4
ASET	490.69	5
UISP	464.16	6
IGP	440.56	7
DICCL	413.47	8
ISFCS	394.75	9
PDACS	366.30	10

Emergent cybersecurity trends: The permanent value of *emergent cybersecurity trends* for experts 1, 2, 3, and 4 are 503, 481, 531, and 556, respectively. Cyber-attacks are inherently complex and evolving occurrences that catch unprepared businesses off-guard [79]. It is necessary to design and implement cybersecurity systems with the flexibility to allow future upgrades [8].

Non-availability of cybersecurity curriculum in education: The permanent value of *non-availability of cybersecurity curriculum in education* for experts 1, 2, 3, and 4 are 504, 446, 528, and 497, accordingly. Catal and Tekinerdogan [76] recommended developing separate courses for Industry 5.0 cybersecurity rather than including cybersecurity with Industry 5.0 technologies like cyber-physical systems, real-time optimization, etc. This approach would allow more focused presentation and study of cybersecurity topics by both students and instructors.

Embedded technical constraints: The permanent value of *embedded technical constraints* for experts 1, 2, 3, and 4 are 478, 439, 490, and 475, respectively. There are some technical obstacles before the implementation of Industry 5.0 cybersecurity; for instance, old devices have fewer capabilities to adopt currently appropriate security measures, inadequate use of modern security techniques such as encryption software, and system supervision software is not completely ready for Industry 5.0 [57,56]. Robust and dependable security measures must be designed to handle diverse Industry 5.0 networks while continuing the use of encryption and authorization. Additionally, system network monitoring must be increased by expanding safety staff and resources [87].

Absence of skilled employees and training: The permanent value of *absence of skilled employees and training* for experts 1, 2, 3, and 4 are 482, 399, 508, and 464, correspondingly. Expertise is an important element for managing the cybersecurity of Industry 5.0. In certain areas, such as the security of smart production systems that have identified deficits, organizations should arrange training programs to increase staff proficiency [8].

Unstandardized Industry 5.0 security policies: The permanent value of *unstandardized Industry 5.0 security policies* for experts 1, 2, 3, and 4 are 474, 442, 504, and 441, respectively. Presently, no smart manufacturing-specific cybersecurity standards are available [8]. Without a standard baseline, system improvement becomes a more difficult and time-consuming task. Analysis of existing security standards should be carried out to identify best practices and possible holes for Industry 5.0 cybersecurity implementation [57].

Insufficient government patronization: The permanent value of *insufficient government patronization* for experts 1, 2, 3, and 4 are 465, 392, 435, and 422, respectively. Government is reluctant to fund research on cybersecurity of Industry 5.0 [73]. All actions must be completely consistent and integrated with national cybersecurity [9].

Deficiency in interoperability and common communication language: The permanent value of *deficiency in interoperability and common communication language* for experts 1, 2, 3, and 4 are 378, 377,432, and 434, respectively. The challenge of interoperability arises with the adoption and integration of Industry 5.0 technologies, interfaces, and platforms into current systems. Ensuring interoperability across equipment and systems is important for both smooth operation and cybersecurity [57].

Insufficient strategy to fund security challenges: The permanent value of *insufficient strategy to fund security* for experts 1, 2, 3, and 4 are 465, 392, 435, and 422, respectively. Organizational leaders have not traditionally favored investment in cybersecurity [46]. Highlighting the potentially devastating economic loss from breaches in contrast with lesser investment in cybersecurity is a favorable approach.

Poorly defined accountability of cybersecurity: The permanent value of *poorly defined accountability of cybersecurity* for experts 1, 2, 3, and 4 are 350, 352, 366, and 390, respectively. Owing to the intrinsic diversity of the network, accountability over the lifecycle of Industry 5.0 security goods is inadequately specified [60]. Effective regulatory procedures are needed to improve both accountability and client assimilation of Industry 5.0 cybersecurity standards and practices [57,59].

5.2. Managerial and educational implications of research

This study provides a priority structure of literature-derived Industry 5.0 cybersecurity challenges using the GTMA method. This analysis may help Industry 5.0 firms and those eager to adopt Industry 5.0 in successfully navigating cybersecurity challenges. These cybersecurity challenges can be met by proper organizational management and governmental support. Other contributions of this study are as follows:

Fig. 17. Overall Priority Ranking of Industry 5.0 Cybersecurity Challenges.

- This study creates a roadmap for strategically addressing the challenges of cybersecurity in Industry 5.0.
- This study helps managers to gain knowledge about the challenges of cybersecurity in Industry 5.0.
- This study provides managers with a hierarchy of cybersecurity challenges that will allow successful concurrent operation and assimilation of appropriate countermeasures.
- This study provides insight into the inter-relationships among key Industry 5.0 cybersecurity challenges and sub-challenges.
- This study will help industry 5.0 policymakers identify the types of issues that should be integrated into cybersecurity systems.

The managerial and educational implications in this study are examined one-by-one as they relate to the identified challenges. The explicit detail of these findings illustrates the current interrelated state of cybersecurity in industry and education. The following implications are presented with recommendations intended to guide the endeavors of industrial firms and educational institutions towards a more productive, sustainable, and secure digital future.

Industry 5.0 supply chain security problems: As Industry 5.0 increases supply chain security exposures, managers should prioritize issues associated with their own expanding interdependence over their suppliers. To reduce the expansive horizontal cybersecurity risk of expanding the supplier base, regular risk evaluations are recommended. This will allow managers to mitigate risk by aligning with vendors that follow industry-accepted security standards and certification programs in addition to safe software development lifecycles [57].

Upgrading of cybersecurity systems: The persistent advancement of cyber-attacks in number and sophistication mandates a commensurate elevation of Industry 5.0 cybersecurity networks. Managers must implement cybersecurity development programs that incorporate aggressive hiring of leading personnel along with university and industry sharing of research and best practices. These elements will help build up-to-date and flexible systems that can cope with the most sophisticated hacking attempts.

Design of effective cybersecurity curricula: Cybersecurity within Industry 5.0-related courses must become mandatory within relevant education programs. This is an area where collaboration between education and industry is necessary to appropriately cope with the fast pace of change within the sector. Diligent work along these lines, while not yielding fast results, will likely be the most effective long-term mitigation of Industry 5.0 cybersecurity risk.

Removal of technical problems: The top technical priority for managers is verifying and modernizing Industry 5.0 devices and systems. Capital spent on advanced monitoring, encryption, and authentication systems will be wasted without the hardware needed to realize their benefits.

Development of effective employee training: The current gap in qualified experts within the Industry 5.0 cybersecurity field can be partially filled by employers investing in on-the-job and off-site training programs. As training programs are developed, they must be maintained and updated to reflect fast-paced changes in technology and approach. Managers should also be conscious of the close interrelation of training and the identified challenge driven by employee difficulties with new Industry 5.0 cybersecurity skills.

Standardization of Industry 5.0 cybersecurity policies: Standards are needed that institutionalize best practices as a baseline for continuous improvement. These must not, however, create local optima at the expense of other system components. Further research is needed to understand how standards may be systematically created and implemented across disparate organizations and inter-organizational functions.

Standardization of operational technologies: Standard interfaces and interfacing technology will allow faster growth of Industry 5.0 technologies. This will also allow cybersecurity managers and practitioners to focus more of their efforts on securing networks rather than simple interconnectivity. The secure integration of IT and OT devices serves as a foundation for the solutions to other Industry 5.0 cybersecurity challenges.

Elicitation of government support: The roles of government within Industry 5.0 cybersecurity are both to fund research as well as to generate effective legislation. Industry and academia must each contribute to these vital endeavors as they are themselves an interdependent system. Governments must be made aware of the criticality of cybersecurity as it relates to the health of national and global economies.

Funding of organizational cybersecurity systems: Managers must overcome the negative stigma associated with cybersecurity investment. As these investments may be difficult to champion without associated profit or product value increases, the development of organizational policy to secure investment is needed. This will protect long-term company interests effected by cyber-attacks.

Development of stakeholder cybersecurity liability policies: Present legislation does not provide a clear delineation of cybersecurity responsibility for product stakeholders. This may create gaps as firms work from disparate understandings of cybersecurity coverage. The increasing technological system complexity of Industry 5.0 is exacerbating this issue. It is, therefore, prudent for legislative bodies to continuously develop and adapt guidelines that define clear roles and responsibilities for all cybersecurity stakeholders.

5.3. Theoretical implications of research

- This study aggregates current cybersecurity challenges within the Industry 5.0 paradigm to create a broader overview than any other research in this field.
- This study is an example of an efficient and effective application of Graph theory and Matrix approach in the Industry 5.0 area and will help practitioners and academics understand the underlying principles and applications to the field of interest.
- From the perspective of industry 5.0, the technique suggested in this study will help decision-makers make an effective choice while considering cybersecurity issues in a variety of disruptive circumstances.
- The suggested approach also provides step-by-step instructions on how to use GTMA to evaluate challenges and sub-challenges; furthermore, it creates a rating of challenges for the dedicated audience and investigators in Industry 5.0.
- By developing a mathematical framework to identify the most significant cybersecurity challenge of Industry 5.0, this work fills in major voids in existing research.

5.4. Policy implications of research

The study identifies that complex supply chains pose the greatest risk to cybersecurity in Industry 5.0. The study also shows that emerging cyber-attacks and the lack of cybersecurity courses in the curriculum are the two main challenges to cybersecurity. Having this information will assist policymakers in prioritizing challenges and taking subsequent countermeasures.

6. Conclusion

The Industry 5.0 paradigm is attractive to many organizations as it increases productivity and sustainability within the manufacturing system. This study has summarized the previously identified cybersecurity challenges and sub-challenges of Industry 5.0. Additionally, the GTMA method has been implemented to fill a research gap by evaluating the challenges and prioritizing the sub-challenges. The resultant data

analyses represent the hierarchy of inter-related challenges based on expert input: supply chain vulnerabilities are the most significant challenge, followed by emergent cybersecurity trends in second place. The rest of the hierarchy, in descending order, is as follows: non-availability of the cybersecurity curriculum in education, embedded technical constraints, absence of skilled employees and training, unstandardized Industry 5.0 security policies, insufficient government patronization, deficiency in interoperability and common communication language, insufficient strategy to fund security, poorly defined accountability of cybersecurity.

For analysis, data was collected from four experts working in Industry 5.0 firms. This study and the analysis contained may help in the future study of Industry 5.0 cybersecurity by providing a robust basis for expansion. Moreover, it can help to influence improved policies and regulations to overcome the serious concerns generated by the advancing and empowering technology of Industry 5.0.

To conclude, four experts were consulted in this study; however, in future studies, the number of experts could be increased or categorized based on specific industries to provide a more robust analysis. This would provide an intriguing opportunity for a more wide-ranging stakeholder perspective on cybersecurity challenges in Industry 5.0. Alternatively, segmenting experts according to specific industries could bolster a more robust analysis, offering an intriguing chance to embrace a broader stakeholder perspective on the cybersecurity challenges of Industry 5.0. While this study has concentrated on the German context's Industry 5.0 cybersecurity challenges, its scope could be broadened in the coming years to encompass other economies such as India, China, and South Africa. Furthermore, the research's horizons could expand by incorporating novel and dynamic countermeasures to surmount these challenges. In sum, this methodology holds potential for application in other facets of Industry 5.0, such as economic hurdles and risk management in the future.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Appendix A

Table A.1

Table A.1
List of abbreviations.

Abbreviations	Full form
GTMA	Graph Theory and Matrix Approach
ASET	Absence of skilled employee and training
ISFCS	Insufficient strategy to fund cybersecurity
PDACS	Poorly Defined Accountability of Cyber-Security
UISPC	Unstandardized Industry 5.0 Security Policies
SCV	Supply Chain Vulnerabilities
DICCL	Deficiency in Interoperability and Common Communication Language
ETC	Embedded Technical Constraints
IGP	Insufficient Government Patronization
NACSCE	Non-availability of Cyber-Security Curriculum in Education
ECST	Emergent Cyber-Security Trends
AI	Artificial Intelligence
MCDM	Multi-Criteria Decision-Making
DEMATEL	Decision making trial and evaluation laboratory
CPS	Cyber-Physical Systems
IoT	Internet of Things
BWM	Best-Worst Method
FMEA	Failure Mode and Effect Analysis
ISM	Interpretative Structural Modelling
TOPSIS	Technique for Order of Preference by Similarity to Ideal Solution
IT	Information Technology

Appendix B

Survey Questionnaire
Dear Sir/Madam,
Greetings. We are conducting research on ranking cybersecurity of Industry 5.0 challenges using graph theory and matrix approach.
If you agree to participate in the research, please fill in the data.
Company:
Designation:
Year of experience:
Objective:

1. Rating sub-challenges based on their impact on challenges using scale from Table B.1.
2. Rating relative importance of sub-challenges.

Here we have listed 30 sub-challenges under 10 challenges from literature.
Part 1: Using the ratings in Table 1, note the presumed impact of each sub-challenge on its related main challenge.

Table B.1
the scale of impact of sub-challenges.

scale of importance	rating (f_i)
Extremely low	1
Low	2
Below average	3
Average	4
Above average	5
High	6
Extremely high	7

Part 2: In this part we collect data on pairwise comparison of sub challenges using the scale found in Table B.2

Table B.2
sub-challenge impact scale.

Description	Relative significance of challenges	
	f_{xy}	$f_{yx} = 10 - f_{xy}$
Comparing challenges are equally significance	5	5
One challenge is moderately important over another	6	4
One challenge is strongly important over another	7	3
One challenge is very strongly important over another	8	2
One challenge is extremely important over another	9	1
One challenge is extraordinarily important over another	10	0

Appendix C

Formula for calculation of matrix permanent

$$
\begin{aligned}
per(M) = {} & \prod_{i=1}^{N} E_i + \sum_{i=1}^{N-1}\sum_{j=i+1}^{N} \ldots\ldots\ldots\ldots \sum_{N=t+1}^{N} \left(f_{ij}f_{ji}\right)E_kE_lE_mE_nE_o\ldots E_tE_N \ \ldots\ldots\ N \neq pus \\
& + \sum_{i=1}^{N-2}\sum_{j=i+1}^{N-1}\sum_{k=j+1}^{N} \ldots\ldots \sum_{N=t+1}^{N} \left(f_{ij}f_{jk}f_{ki} + f_{ik}f_{kj}f_{ji}\right)E_lE_mE_nE_o\ldots E_tE_N \ k\ldots\ldots N \neq pus \\
& + \sum_{i=1}^{N-3}\sum_{j=i+1}^{N}\sum_{k=i+2}^{N-1}\sum_{l=i+2}^{N} \ldots\ldots \sum_{N=t+1}^{N} \left(f_{ij}f_{ji}\right)\left(f_{kl}f_{lk}\right)E_mE_nE_o\ldots\ldots E_tE_N \ k,l\ldots\ldots N \neq pus \\
& + \sum_{i=1}^{N-3}\sum_{j=i+1}^{N+1}\sum_{k=i+1}^{N}\sum_{l=i+1}^{N} \ldots\ldots \sum_{N=t+1}^{N} \left(f_{ij}f_{jk}f_{kl}f_{li} + f_{il}f_{lk}f_{kj}f_{ji}\right)E_mE_nE_o\ldots\ldots E_tE_N \ k,l\ldots\ldots N \neq pus \\
& + \sum_{i=1}^{N-2}\sum_{j=i+1}^{N-1}\sum_{k=j+1}^{N}\sum_{l=1}^{N-1}\sum_{m=l+1}^{N} \ldots \sum_{N=t+1}^{N} \left(f_{ij}f_{jk}f_{ki} + f_{ik}f_{kj}f_{ji}\right)\left(f_{lm}f_{ml}\right)E_nE_o\ldots E_tE_N \ k,l,m\ldots\ldots N \neq pus \\
& + \sum_{i=1}^{N-4}\sum_{j=i+1}^{N-1}\sum_{k=j+1}^{N}\sum_{l=i+1}^{N-1}\sum_{m=j+1}^{N} \ldots \sum_{N=t+1}^{N} \left(f_{ij}f_{jk}f_{kl}f_{lm}f_{mi} + f_{im}f_{ml}f_{lk}f_{kj}f_{ji}\right)E_nE_o..E_tE_N \ k,l,m..N \neq pus \\
& + \sum_{i=1}^{N-5}\sum_{j=i+1}^{N-1}\sum_{k=j+1}^{N}\sum_{l=1}^{N-2}\sum_{m=l+1}^{N-1}\sum_{n=m+1}^{N} \ldots \sum_{N=t+1}^{N} \left(f_{ij}f_{jk}f_{ki} + f_{ik}f_{kj}f_{ji}\right)\left(f_{lm}f_{mn}f_{nl} + f_{lm}f_{nm}f_{ml}\right)E_o..E_tE_N \ k,l,m,n\ldots\ldots N \neq pus \\
& + \sum_{i=1}^{N-5}\sum_{j=i+1}^{N}\sum_{k=i+1}^{N-3}\sum_{l=i+2}^{N}\sum_{m=k+1}^{N-1}\sum_{n=k+1}^{N} \ldots \sum_{N=t+1}^{N} \left(f_{ij}f_{ji}\right)\ \left(f_{kl}f_{lk}f_{ji}\right)\left(f_{mn}f_{nm}\right)E_o..E_tE_N \ k,l,m,n\ldots N \neq pus \\
& + \sum_{i=1}^{N-5}\sum_{j=i+1}^{N-1}\sum_{k=i+1}^{N}\sum_{l=i+1}^{N}\sum_{m=i+1}^{N}\sum_{n=j+1}^{N} \ldots \sum_{N=t+1}^{N} \left(f_{ij}f_{jk}f_{kl}f_{lm}f_{mn}f_{in} + f_{ni}f_{nm}f_{ml}f_{lk}f_{kj}f_{ji}\right)\ E_o..E_tE_N \ k,l,m,n\ldots N \neq pus
\end{aligned}
\tag{C.1}
$$

Permanent calculations for sub-challenge VPMs by Expert
Insufficient strategy to fund security permanent values based on Expert data are as follows:

$$Permanent^{Expert1}(ISFCS) = \begin{bmatrix} 2 & 4 & 3 \\ 6 & 3 & 3 \\ 7 & 7 & 2 \end{bmatrix} = 375$$

$$Permanent^{Expert2}(ISFCS) = \begin{bmatrix} 2 & 3 & 3 \\ 7 & 3 & 4 \\ 7 & 6 & 1 \end{bmatrix} = 378$$

$$Permanent^{Expert3}(ISFCS) = \begin{bmatrix} 3 & 4 & 4 \\ 6 & 3 & 3 \\ 6 & 7 & 1 \end{bmatrix} = 408$$

$$Permanent^{Expert4}(ISFCS) = \begin{bmatrix} 3 & 4 & 4 \\ 6 & 2 & 5 \\ 6 & 5 & 2 \end{bmatrix} = 411$$

Permanent values of *poorly defined accountability of cybersecurity* matrices based on data provided by experts are the following:

$$Permanent^{Expert1}(PDACS) = \begin{bmatrix} 2 & 5 & 5 \\ 5 & 1 & 6 \\ 5 & 4 & 1 \end{bmatrix} = 350$$

$$Permanent^{Expert2}(PDACS) = \begin{bmatrix} 2 & 5 & 5 \\ 5 & 1 & 5 \\ 5 & 5 & 1 \end{bmatrix} = 352$$

$$Permanent^{Expert3}(PDACS) = \begin{bmatrix} 2 & 6 & 6 \\ 4 & 2 & 5 \\ 4 & 5 & 1 \end{bmatrix} = 366$$

$$Permanent^{Expert4}(PDACS) = \begin{bmatrix} 2 & 5 & 4 \\ 5 & 1 & 7 \\ 6 & 3 & 2 \end{bmatrix} = 390$$

Permanent values of *unstandardized Industry 5.0 policies* matrices based on data provided by experts are as follows:

$$Permanent^{Expert1}(UISP) = \begin{bmatrix} 2 & 7 & 4 \\ 3 & 3 & 6 \\ 6 & 4 & 2 \end{bmatrix} = 474$$

$$Permanent^{Expert2}(UISP) = \begin{bmatrix} 2 & 6 & 4 \\ 4 & 2 & 5 \\ 6 & 5 & 3 \end{bmatrix} = 442$$

$$Permanent^{Expert3}(UISP) = \begin{bmatrix} 3 & 9 & 5 \\ 1 & 3 & 7 \\ 5 & 3 & 2 \end{bmatrix} = 504$$

$$Permanent^{Expert4}(UISP) = \begin{bmatrix} 2 & 8 & 5 \\ 2 & 3 & 5 \\ 5 & 5 & 2 \end{bmatrix} = 441$$

Permanent values of *supply chain vulnerabilities* based on data provided by experts are the following:

$$Permanent^{Expert1}(SCV) = \begin{bmatrix} 5 & 5 & 7 \\ 5 & 3 & 6 \\ 3 & 4 & 3 \end{bmatrix} = 533$$

$$Permanent^{Expert2}(SCV) = \begin{bmatrix} 6 & 5 & 7 \\ 5 & 2 & 5 \\ 3 & 5 & 3 \end{bmatrix} = 553$$

$$Permanent^{Expert3}(SCV) = \begin{bmatrix} 4 & 5 & 3 \\ 5 & 3 & 6 \\ 7 & 4 & 4 \end{bmatrix} = 577$$

$$Permanent^{Expert4}(SCV) = \begin{bmatrix} 5 & 6 & 5 \\ 4 & 4 & 5 \\ 5 & 5 & 3 \end{bmatrix} = 607$$

Permanent values of *deficiency in interoperability and common communication language* based on data provided by experts are the following:

$$Permanent^{Expert1}(DICCL) = \begin{bmatrix} 2 & 8 & 5 \\ 2 & 2 & 4 \\ 5 & 6 & 3 \end{bmatrix} = 378$$

$$Permanent^{Expert2}(DICCL) = \begin{bmatrix} 3 & 7 & 5 \\ 3 & 2 & 3 \\ 5 & 7 & 2 \end{bmatrix} = 377$$

$$Permanent^{Expert3}(DICCL) = \begin{bmatrix} 4 & 7 & 6 \\ 3 & 3 & 4 \\ 4 & 6 & 2 \end{bmatrix} = 432$$

$$Permanent^{Expert4}(DICCL) = \begin{bmatrix} 3 & 6 & 5 \\ 4 & 3 & 3 \\ 5 & 7 & 2 \end{bmatrix} = 434$$

Permanent values of *embedded technical constraints* based on data provided experts are the following:

$$Permanent^{Expert1}(ETC) = \begin{bmatrix} 2 & 6 & 4 \\ 4 & 2 & 3 \\ 6 & 7 & 6 \end{bmatrix} = 478$$

$$Permanent^{Expert2}(ETC) = \begin{bmatrix} 2 & 5 & 3 \\ 5 & 2 & 3 \\ 7 & 7 & 5 \end{bmatrix} = 439$$

$$Permanent^{Expert3}(ETC) = \begin{bmatrix} 2 & 8 & 4 \\ 2 & 3 & 5 \\ 6 & 5 & 4 \end{bmatrix} = 490$$

$$Permanent^{Expert4}(ETC) = \begin{bmatrix} 3 & 6 & 8 \\ 4 & 3 & 5 \\ 2 & 5 & 4 \end{bmatrix} = 475$$

Permanent values of *insufficient government patronization* based on data provided Expert data are the following:

$$Permanent^{Expert1}(IGP) = \begin{bmatrix} 2 & 5 & 6 \\ 5 & 3 & 5 \\ 4 & 5 & 3 \end{bmatrix} = 465$$

$$Permanent^{Expert2}(IGP) = \begin{bmatrix} 1 & 4 & 5 \\ 6 & 2 & 6 \\ 5 & 4 & 3 \end{bmatrix} = 392$$

$$Permanent^{Expert3}(IGP) = \begin{bmatrix} 3 & 6 & 7 \\ 4 & 2 & 7 \\ 3 & 3 & 4 \end{bmatrix} = 435$$

$$Permanent^{Expert4}(IGP) = \begin{bmatrix} 2 & 6 & 6 \\ 4 & 3 & 5 \\ 4 & 5 & 2 \end{bmatrix} = 422$$

Permanent values of *non-availability of cybersecurity curriculum in education* based on data provided by four Expert data are the following:

$$Permanent^{Expert1}(NACSCE) = \begin{bmatrix} 4 & 8 & 6 \\ 2 & 3 & 3 \\ 4 & 7 & 6 \end{bmatrix} = 504$$

$$Permanent^{Expert2}(NACSCE) = \begin{bmatrix} 5 & 8 & 5 \\ 2 & 2 & 2 \\ 5 & 8 & 6 \end{bmatrix} = 446$$

$$Permanent^{Expert3}(NACSCE) = \begin{bmatrix} 4 & 8 & 7 \\ 2 & 4 & 8 \\ 3 & 2 & 5 \end{bmatrix} = 528$$

$$Permanent^{Expert4}(NACSCE) = \begin{bmatrix} 4 & 8 & 7 \\ 2 & 3 & 7 \\ 3 & 3 & 5 \end{bmatrix} = 497$$

Permanent values of matrices of *difficult to face emerging cybersecurity trends* based on data provided by four Expert data are the following:

$$Permanent^{Expert1}(ECST) = \begin{bmatrix} 3 & 6 & 4 \\ 4 & 2 & 5 \\ 6 & 5 & 4 \end{bmatrix} = 503$$

$$Permanent^{Expert2}(ECST) = \begin{bmatrix} 3 & 5 & 2 \\ 5 & 2 & 5 \\ 8 & 5 & 4 \end{bmatrix} = 481$$

$$Permanent^{Expert3}(ECST) = \begin{bmatrix} 5 & 8 & 8 \\ 2 & 5 & 9 \\ 2 & 1 & 5 \end{bmatrix} = 490$$

$$Permanent^{Expert4}(ECST) = \begin{bmatrix} 4 & 7 & 7 \\ 3 & 3 & 6 \\ 3 & 4 & 4 \end{bmatrix} = 501$$

References

[1] S. Huang, B. Wang, X. Li, P. Zheng, D. Mourtzis, L. Wang, Industry 5.0 and Society 5.0—Comparison, complementation and co-evolution, J. Manuf. Syst. 64 (2022) 424–428.

[2] X. Xu, Y. Lu, B. Vogel-Heuser, L. Wang, Industry 4.0 and Industry 5.0—Inception, conception and perception, J. Manuf. Syst. 61 (2021) 530–535.

[3] J. Qin, Y. Liu, R. Grosvenor, A categorical framework of manufacturing for industry 4.0 and beyond, Procedia CIRP. 52 (2016) 173–178.

[4] M.A. Moktadir, S.M. Ali, S. Kusi-Sarpong, M.A.A. Shaikh, Assessing challenges for implementing Industry 4.0: implications for process safety and environmental protection, Process Safet. Environ. Protect. 117 (2018) 730–741.

[5] M. Breque, L. De Nul, A. Petridis, Industry 5.0: Towards a Sustainable, Human Centric and Resilient European Industry, Publications Office, UN, 2021. https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/industry-50-towards-sustainable-human-centric-and-resilient-european-industry_en.

[6] S.R. Chhetri, S. Faezi, N. Rashid, M.A. Al Faruque, Manufacturing supply chain and product lifecycle security in the era of industry 4.0, J. Hardware . Syst. Secu. 2 (1) (2018) 51–68.

[7] A. Corallo, M. Lazoi, M. Lezzi, A. Luperto, Cybersecurity awareness in the context of the Industrial Internet of Things: a systematic literature review, Comput. Indu. 137 (2022) 103614.

[8] N. Tuptuk, S. Hailes, Security of smart manufacturing systems, J. Manuf. Syst. 47 (2018) 93–106.
[9] B.C. Ervural, B. Ervural, Overview of cyber security in the industry 4.0 era. Industry 4.0: Managing the Digital Transformation, Springer, 2018, pp. 267–284.
[10] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, N. Meskin, Cybersecurity for industrial control systems: a survey, Comput. Sec. 89 (2020) 101677.
[11] S.V. Bharathi, Prioritizing and ranking the big data information security risk spectrum, Glob. J. Flexible Syst. Manage. 18 (3) (2017) 183–201.
[12] S. Tweneboah-Koduah, K.E. Skouby, R. Tadayoni, Cyber security threats to IoT applications and service domains, Wirel. Pers. Commun. 95 (1) (2017) 169–185.
[13] Kaspersky Lab, The Human Factor in IT security: How employees Are Making Businesses Vulnerable from Within, Kaspersky, 2018.
[14] Malatras, A., Stanic, Z., Lella, I., De Sousa Figueiredo, R., Tsekmezoglou, E., Theocharidou, M., ... & Drougkas, A. (2023). ENISA threat landscape: transport Sector (January 2021 to October 2022), https://doi.org/10.2824/553997.
[15] Bada, M., Sasse, A.M., & Nurse, J.R. (2019). Cyber security awareness campaigns: why do they fail to change behaviour?. arXiv preprint arXiv:1901.02672.
[16] K. Khando, S. Gao, S.M. Islam, A. Salman, Enhancing employees information security awareness in private and public organisations: a systematic literature review, Comput. Secur. 106 (2021) 102267.
[17] W. He, Z. Zhang, Enterprise cybersecurity training and awareness programs: recommendations for success, J. Organizat. Comput. Electronic Commerce 29 (4) (2019) 249–257.
[18] S.A. Fazio, *A dual perspective towards building resilience in manufacturing organizations*, Mississippi State University (2021).
[19] T. Zheng, M. Ardolino, A. Bacchetti, M. Perona, The applications of Industry 4.0 technologies in manufacturing context: a systematic literature review, Int. J. Prod. Res. 59 (6) (2021) 1922–1954.
[20] Praveen Kumar Reddy Maddikunta, Quoc-Viet Pham, B. Prabadevi, N. Deepa, Kapal Dev, Thippa Reddy Gadekallu, Rukhsana Ruby, Madhusanka Liyanage, Industry 5.0: a Survey on Enabling Technologies and Potential Applications, J. Ind. Inf. Integr. 26 (2022) 100257, https://doi.org/10.1016/j.jii.2021.100257.
[21] S. Vaidya, P. Ambad, S. Bhosle, Industry 4.0–a glimpse, Procedia Manuf. 20 (2018) 233–238.
[22] H. Lasi, P. Fettke, H.G. Kemper, T. Feld, M. Hoffmann, Industry 4.0, Bus. Inform. Syst. Eng. 6 (4) (2014) 239–242.
[23] S. Rahman, N.U.I. Hossain, K. Govindan, F. Nur, M. Bappy, Assessing cyber resilience of additive manufacturing supply chain leveraging data fusion technique: a model to generate cyber resilience index of a supply chain, CIRP. J. Manuf. Sci. Technol. 35 (2021) 911–928.
[24] N.U.I. Hossain, S. Rahman, S.A. Liza, Cyber-susiliency index: a comprehensive resiliency-sustainability-cybersecurity index for healthcare supply chain networks, Decis. Anal. J. 9 (2023) 100319.
[25] V. Jesus, M. Josephs, Innovation in manufacturing through digital technologies and applications: thoughts and Reflections on Industry 4.0. Thoughts Reflect. Indust. 4.0, 2018, pp. 61–70.
[26] M. Johnson, R. Jain, P. Brennan-Tonetta, E. Swartz, D. Silver, J. Paolini, C. Hill, Impact of big data and artificial intelligence on industry: developing a workforce roadmap for a data driven economy, Glob. J. Flexib. Syst. Manage. 22 (3) (2021) 197–217.
[27] P.K. Malik, R. Sharma, R. Singh, A. Gehlot, S.C. Satapathy, W.S. Alnumay, D. Pelusi, U. Ghosh, J. Nayak, Industrial internet of things and its applications in industry 4.0: state of the art, Comput. Commun. 166 (2021) 125–139.
[28] J. Lee, B. Bagheri, H.A. Kao, A cyber-physical systems architecture for industry 4.0-based manufacturing systems, Manuf. Lett. 3 (2015) 18–23.
[29] M.T. Taghavifard, S. Majidian, Identifying cloud computing risks based on firm's ambidexterity performance using fuzzy VIKOR technique, Glob. J. Flexi. Syst. Manage. 23 (1) (2022) 113–133.
[30] A. Haleem, M. Javaid, Additive manufacturing applications in industry 4.0: a review, J. Indust. Integrat. Manage. 4 (04) (2019) 1930001.
[31] G.M. Santi, A. Ceruti, A. Liverani, F. Osti, Augmented reality in industry 4.0 and future innovation programs, Technol.. (Basel) 9 (2) (2021) 33.
[32] J.V.D. Ham, Toward a better understanding of "cybersecurity", Digit. Threats: Res. Pract. 2 (3) (2021) 1–3.
[33] T. Sawik, A linear model for optimal cybersecurity investment in Industry 4.0 supply chains, Int. J. Prod. Res. 60 (4) (2022) 1368–1385.
[34] M. Lezzi, M. Lazoi, A. Corallo, Cybersecurity for Industry 4.0 in the current literature: a reference framework, Comput. Ind. 103 (2018) 97–110.
[35] J. Prinsloo, S. Sinha, B. von Solms, A review of industry 4.0 manufacturing process security risks, Appl. Sci. 9 (23) (2019) 5105.
[36] T. Sobb, B. Turnbull, N. Moustafa, Supply chain 4.0: a survey of cyber security challenges, solutions and future directions, Electronics (Basel) 9 (11) (2020) 1864.
[37] A. Finance, Industry 4.0 Challenges and solutions for the digital transformation and use of exponential technologies, Finance, Audit Tax Consul. Corporate: Zurich, Swiss (2015) 1–12.
[38] I. Ahmed, M.N. Shupti, S. Islam, N.U.I. Hossain, A.M. Sokolov, Application of system modeling language (SysML) in cyber level architecture of industry 4.0, in: Proceedings of the International Annual Conference of the American Society for Engineering Management, American Society for Engineering Management (ASEM), 2022, pp. 1–9.
[39] M.N. Shupti, I. Ahmed, N.U.I. Hossain, A.M. Sokolov, G. Kannan, K. Babski-Reeves, Leveraging Systems Modeling Language (SysML) in Configuration Level of the 5C Architecture, in: Proceedings of the International Annual Conference of the American Society for Engineering Management, American Society for Engineering Management (ASEM), 2021, pp. 1–9.
[40] I. Ilhan, M. Karaköse, Cybersecurity framework for requirements of repair, update, and renovation in industry 4.0, in: 2019 1st international informatics and software engineering conference (UBMYK), IEEE, 2019, pp. 1–4.
[41] P. Radanliev, D. De Roure, J.R. Nurse, R. Nicolescu, M. Huth, S. Cannady, R. M. Montalvo, Integration of cyber security frameworks, models and approaches for building design principles for the internet-of-things in industry 4.0. Living in the Internet of Things: Cybersecurity of the IoT-2018, IET, 2018, pp. 1–6.
[42] I.H. Sarker, M.H. Furhad, R. Nowrozy, Ai-driven cybersecurity: an overview, security intelligence modeling and research directions, SN. Comput. Sci. 2 (3) (2021) 1–18.
[43] A.A. Süzen, A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem, Int. J.f Comput. Netw. Inform. Sec. 12 (1) (2020).
[44] T. Pereira, L. Barreto, A. Amaral, Network and information security challenges within Industry 4.0 paradigm, Procedia Manuf. 13 (2017) 1253–1260.
[45] N. Benias, A.P. Markopoulos, A review on the readiness level and cyber-security challenges in Industry 4.0, in: 2017 South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), IEEE, 2017, pp. 1–5.
[46] G. Culot, F. Fattori, M. Podrecca, M. Sartor, Addressing industry 4.0 cybersecurity challenges, IEEE Eng. Manage. Rev. 47 (3) (2019) 79–86.
[47] A.A. Mukherjee, A. Raj, S. Aggarwal, Identification of barriers and their mitigation strategies for industry 5.0 implementation in emerging economies, Int. J. Prod. Econ. (2023) 108770.
[48] C.L. Karmaker, A.M. Bari, M.Z. Anam, T. Ahmed, S.M. Ali, Jesus de, D.A. Pacheco, M.A. Moktadir, Industry 5.0 challenges for post-pandemic supply chain sustainability in an emerging economy, Int. J. Prod. Econ. 258 (2023) 108806.
[49] M. Ghobakhloo, M. Iranmanesh, M.F. Mubarak, M. Mubarik, A. Rejeb, M. Nilashi, Identifying industry 5.0 contributions to sustainable development: a strategy roadmap for delivering sustainability values, Sustain. Prod. Consum. 33 (2022) 716–737.
[50] S.M. Ali, S.N. Hoq, A.M. Bari, G. Kabir, S.K. Paul, Evaluating factors contributing to the failure of information system in the banking industry, PLoS ONE 17 (3) (2022) e0265674.
[51] S. Parker, Z. Wu, P.D. Christofides, Cybersecurity in process control, operations, and supply chain, Comput. Chem. Eng. (2023) 108169.
[52] D. Banik, N.U.I. Hossain, K. Govindan, F. Nur, K. Babski-Reeves, A decision support model for selecting unmanned aerial vehicle for medical supplies: context of COVID-19 pandemic, Int. J. Logist. Manage. 34 (2) (2022) 473–496.
[53] M. Singh, I.A. Khan, S. Grover, Selection of manufacturing process using graph theoretic approach, Int. J. Syst. Assur. Eng. Manage. 2 (4) (2011) 301–311.
[54] S. Wang, J. Wan, D. Li, C. Zhang, Implementing smart factory of industrie 4.0: an outlook, Int. J. Distrib. Sens. Netw. 12 (1) (2016) 3159805.
[55] S.K. Mangla, Y.K. Sharma, P.P. Patil, G. Yadav, J. Xu, Logistics and distribution challenges to managing operations for corporate sustainability: study on leading Indian diary organizations, J. Clean. Prod. 238 (2019) 117620.
[56] A.U. Mentsiev, E.R. Guzueva, T.R. Magomaev, Security challenges of the Industry 4.0, in: Journal of Physics: Conference Series 1515, IOP Publishing, 2020 032074.
[57] A. Malatras, C. Skouloudi, A. Koukounas, Industry 4.0 cybersecurity: challenges & recommendations, Eur. Union Agency Cybersecu. 20 (2019). https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations.
[58] H. Kagermann, Change through digitization—Value creation in the age of Industry 4.0. Management of Permanent Change, Springer, 2015, pp. 23–45.
[59] K.M. Weber, N. Gudowsky, G. Aichholzer, Foresight and technology assessment for the Austrian parliament—Finding new ways of debating the future of industry 4.0, Futures 109 (2019) 240–251.
[60] V. Sklyar, V. Kharchenko, ENISA documents in cybersecurity assurance for industry 4.0: iIoT threats and attacks scenarios, in: 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) 2, IEEE, 2019, pp. 1046–1049.
[61] L.M. Fonseca, Industry 4.0 and the digital society: concepts, dimensions and envisioned benefits, in: Proceedings of the international conference on business excellence 12, 2018, pp. 386–397.
[62] C Schröder, The Challenges of Industry 4.0 For Small and Medium-Sized Enterprises, Friedrich-Ebert-Stiftung, Bonn, Germany, 2016.
[63] F.d.C. Martins, A.T. Simon, R.S.d.J.G. Campos, Produção, Supply Chain 5.0 challenges, Gestão Produção (2020) 27.
[64] S.K. Mangla, P. Kumar, M.K. Barua, Flexible decision approach for analysing performance of sustainable supply chains under risks/uncertainty, Global J. Flexib. Syst. Manage. 15 (2) (2014) 113–130.
[65] S. Luthra, S.K. Mangla, Evaluating challenges to Industry 4.0 initiatives for supply chain sustainability in emerging economies, Process Safety Environ. Protect. 117 (2018) 168–179.
[66] H. He, C. Maple, T. Watson, A. Tiwari, J. Mehnen, Y. Jin, B. Gabrys, The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence, in: 2016 IEEE congress on evolutionary computation (CEC), IEEE, 2016, pp. 1015–1021.
[67] G. Pedone, I. Mezgár, Model similarity evidence and interoperability affinity in cloud-ready Industry 4.0 technologies, Comput. Ind. 100 (2018) 278–286.
[68] L.D. Xu, E.L. Xu, L. Li, Industry 4.0: state of the art and future trends, Int. J. Prod. Res. 56 (8) (2018) 2941–2962.
[69] F. Fraile, T. Tagawa, R. Poler, A. Ortiz, Trustworthy industrial IoT gateways for interoperability platforms and ecosystems, IEEE Internet Things J. 5 (6) (2018) 4506–4514.

[70] J.E. Rubio, R. Roman, J. Lopez, Analysis of cybersecurity threats in industry 4.0: the case of intrusion detection, in: International conference on critical information infrastructures security, Springer, 2017, pp. 119–130.
[71] G. Manogaran, C. Thota, D. Lopez, R. Sundarasekar, Big data security intelligence for healthcare industry 5.0. Cybersecurity For Industry 4.0, Springer, 2017, pp. 103–126.
[72] R. Waslo, T. Lewis, R. Hajj, R. Carton, Industry 5.0 and cybersecurity: managing risk in an age of connected production, Deloitte Insights (2017). Retrieved from: https://www2.deloitte.com/content/dam/insights/us/articles/3749_Industry4-0_cybersecurity/DUP_Industry4-0_cybersecurity.pdf.
[73] E.K. Zervoudi, Fourth industrial revolution: opportunities, challenges, and proposed policies, Indu. Robot.-New Parad. (2020).
[74] Limba, T., Stankevičius, A., & Andrulevičius, A. (2019). Industry 4.0 and national security: the phenomenon of disruptive technology.
[75] M. Hernandez-de-Menendez, C.A. Escobar Díaz, R. Morales-Menendez, Engineering education for smart 4.0 technology: a review, Int. J. Interact. Des. Manuf. (IJIDeM) 14 (3) (2020) 789–803.
[76] C. Catal, B. Tekinerdogan, Aligning education for the life sciences domain to support digitalization and industry 4.0, Procedia Comput. Sci. 158 (2019) 99–106.
[77] T.M. Fernández-Caramés, P. Fraga-Lamas, Use case based blended teaching of IIoT cybersecurity in the industry 5.0 era, Appl. Sci. 10 (16) (2020) 5607.
[78] E.C. ATEŞ, E. BOSTANCI, M.S GÜZEL, Security evaluation of industry 4.0: understanding industry 4.0 on the basis of crime, big data, internet Of Thing (IoT) and cyber physical systems, in: International Security Congress Special Issue, 2020, pp. 29–50.
[79] P.R. Brandao, Bases, challenges, and main Dangers for deploying cybersecurity in industry 4.0, Adv. Wireless Commun. Netw. 5 (1) (2019) 33.
[80] M.M. Bappy, S.M. Ali, G. Kabir, S.K. Paul, Supply chain sustainability assessment with Dempster-Shafer evidence theory: implications in cleaner production, J. Clean. Prod. 237 (2019) 117771.
[81] M. Darvish, M. Yasaei, A. Saeedi, Application of the graph theory and matrix methods to contractor ranking, Int. J. Project Manage. 27 (6) (2009) 610–619.
[82] R.V. Rao, A material selection model using graph theory and matrix approach, Mater. Sci. Eng.: A 431 (1–2) (2006) 248–255.
[83] O.P. Gandhi, V.P. Agrawal, K.S. Shishodia, Reliability analysis and evaluation of systems, Reliab. Eng. Syst. Saf. 32 (3) (1991) 283–305, https://doi.org/10.1016/0951-8320(91)90004-Q.
[84] O.P. Gandhi, V.P. Agrawal, FMEA-A diagraph and matrix approach, Reliab. Eng. Syst. Saf. 35 (2) (1992) 147–158, https://doi.org/10.1016/09518320(92)90034-I.
[85] S. Agrawal, R.K. Singh, Q. Murtaza, Disposition decisions in reverse logistics: graph theory and matrix approach, J. Clean. Prod. 137 (2016) 93–104.
[86] Forbert, H., & Marx, D. (2003). Calculation of the permanent of a sparse positive matrix. 150(3), 267–273.
[87] K. Zhou, T. Liu, L. Liang, From cyber-physical systems to Industry 4.0: make future manufacturing become possible, Int. J. Manuf. Res. 11 (2) (2016) 167–188.