Review

Not peer-reviewed version

Railroad Cybersecurity: A Systematic Bibliometric Review

Ruhaimatu Abudu , Raj Bridgelall * , Bright Parker Quayson , Denver Tolliver , Kwabena Dadson

Posted Date: 12 December 2024

doi: 10.20944/preprints202412.1013.v1

Keywords: bibliometric analysis; cyberthreat; cybersecurity; rail freight; risk; safety; security

 doi:10.20944/preprints202412.1013.v1

Review

Railroad Cybersecurity: A Systematic Bibliometric Review

Ruhaimatu Abudu [1], Raj Bridgelall [1,*], Bright Quayson [1], Denver Tolliver [2] and Kwabena Dadson [1]

[1] Department of Transportation and Supply Chain, College of Business, North Dakota State University, P.O. Box 6050, Fargo, ND 58108-6050, USA
[2] Upper Great Plains Transportation Institute, North Dakota State University, P.O. Box 6050, Fargo, ND 58108-6050, USA
* Correspondence: raj@bridgelall.com or raj.bridgelall@ndsu.edu

Abstract: Cybersecurity challenges are increasing in the rail industry because of constant technological evolution that includes the Internet-of-Things, blockchains, automation, and artificial intelligence. Consequently, many railroads and supply chain stakeholders have implemented strategies and practices to address these challenges. However, the pace of cybersecurity implementation in the railroad industry is slow even as cyberthreats escalate. This systematic review incorporates bibliometric analysis to analyze 70 articles focusing on cybersecurity practices in the rail freight industry, structured around four research questions relating to: (1) challenges, (2) measures, (3) emerging trends, and (4) innovations. Key findings are that implementing cybersecurity practices in the rail freight industry comes with numerous challenges and risks. The study concludes that new threats will constantly emerge with technological advancements. Therefore, there is a need for continuous human training, collaboration, and coordination with stakeholders. This study also highlights research gaps and recommends how stakeholders can most appropriately execute cybersecurity strategies and best coordinate them with the various technological functions in the rail freight industry.

Keywords: bibliometric analysis; cyberthreat; cybersecurity; rail freight; risk; safety; security

1. Introduction

The railroad industry, a crucial backbone of the global supply chain, has been grappling with complex security issues. These complexities are related to the physical infrastructure, human resources, and the intricacies of modern technologies that support modern rail operations. These include Internet-of-Things (IoT) devices, global positioning systems (GPS), and intelligent sensors. For instance, the recent addition of a positive train control (PTC) system has been a critical achievement toward improving safety in this industry [1]. However, these technologies have also opened new vulnerabilities for potential cyberthreats [2]. Cybersecurity in rail freight transportation has become crucial because of the industry's growing dependence on digitalization, connected systems, and automation. For example, malware attacks in the railroad industry have increased by more than 200% globally in the last five years [3]. Although extant studies have explored several areas of railroad cybersecurity, including signaling [4] and cryptographic protocols [5], most of these studies fail to provide a comprehensive perspective on technological, human, and operational risks in railroad cybersecurity. Several of these studies also fail to provide practical mitigation strategies for holistic adaptation. This study aims to bridge this gap by synthesizing findings and recommendations across various domains by offering a comprehensive framework while providing a practical strategy for the growing discourse. Advancing technology in the rail industry heightens the need for robust cybersecurity measures to ensure continuous operations [6]. In addressing these issues, studies focused on various aspects of cybersecurity practices for the rail freight industry, including sustainability [7, 8], risk assessment and management [9], cybersecurity framework [3], and technology innovation [10]. The Transportation Security Administration (TSA) recently implemented a new rule for cybersecurity evaluation of the major modes of transportation, including rail freight

 doi:10.20944/preprints202412.1013.v1

[11]. Although this regulation aims to enhance cyber resilience, some industry stakeholders have raised concerns about its implementation and the associated compliance costs [12].

In the past, transportation security risks mostly stemmed from physical attacks. After 9/11, there was a notable change in focus toward securing transportation systems from potential terrorist threats, leading to comprehensive policies implemented at both national and international levels. This age saw notable advancements in transportation security due to incorporating digital technologies, which brought new vulnerabilities [13]. The railway industry has encountered difficulties in modifying current safety protocols to effectively manage these cybersecurity threats [14]. The literature has identified signaling and communication networks in railway systems as being susceptible to a range of cyberthreats. Other studies highlight vulnerabilities in the sector, including malware, wireless attacks, and unauthorized system access [15]. Initiatives like Shift2Rail [14] and standards developed by international bodies like the International Organization for Standardization [16, 17] and National Institute of Standards and Technology [18, 17] have aimed to enhance cybersecurity resilience in railroad operations. These efforts emphasize the importance of digital security in sustaining operational efficiency and environmental compliance [19]. Demiridis and Pyrgidis (2022) highlighted the significance of cybersecurity in the rail freight sector for sustainable development [20]. The study shows the importance of improving essential services in this industry, such as ensuring high reliability and punctuality to increase competitiveness with other modes of transportation. Aminzadegan et al. (2022) highlighted the environmental friendliness of rail as compared with other modes of transportation [21], making it a priority for government and other policymakers. Rail freight transportation is advancing by integrating digital platforms such as online exchanges [22], making cybersecurity crucial for protecting data and transactions.

This research provides a comprehensive overview of current cybersecurity practices in the rail freight industry through a combined systematic literature review (SLR) and a bibliometric analysis. This **contribution** highlights existing gaps and offers new insights to bridge these gaps. These insights will strengthen the rail freight sector's defenses against current and emerging cyber hazards and open new research opportunities to enhance the industry's cybersecurity. Given the continuous increase in cybersecurity issues in rail freight transportation, this review provides a multifaceted exploration by answering the following four research questions:

1. Challenges: What are the primary cybersecurity threats and vulnerabilities identified in rail freight transportation systems?
2. Measures: How do existing cybersecurity measures address the risks associated with rail freight transportation?
3. Emerging Trends: What are the emerging trends in cybersecurity technologies and practices for enhancing the safety and security of rail freight transportation?
4. Innovation: How effective are current cybersecurity practices in mitigating the risk of cyberattacks in rail transportation networks?

The subsequent sections of this paper are as follows. Section 2 describes the SLR methodology. Section 3 offers answers to the research questions based on the reviewed literature. Section 4 discusses the results while offering implications. Section 5 concludes the SLR, highlighting the gaps identified, limitations, and recommendations for future research.

2. Methodology

Undertaking a literature review is a complex process, with many methods available to compare and contrast the knowledge and gaps in existing literature for a particular set of research questions. These methods range from a traditional literature search, forward or snowball sampling of systematic reviews, and meta-analysis to distill trends. However, the most common contemporary guideline used is the "preferred reporting items for systematic reviews and meta-analyses" (PRISMA), which provides a degree of standardization as compared with others [23]. The authors chose the SLR method over others like narrative, critical, and theoretical reviews for its ability to minimize bias and limitations [24]. The SLR methodology along with the PRISMA checklist systematically identifies research gaps and provides a comprehensive and transparent review approach to evidence synthesis [25]. The PRISMA method comprises 27 items across seven sections, which this study divides into

 doi:10.20944/preprints202412.1013.v1

four stages: the pre-literature collection, literature (publication) selection, systematic review, and data analysis. The authors selected PRISMA to ensure rigor and minimize biases in synthesizing a comprehensive analysis of existing studies. By following the structured stages, the study identifies critical gaps in railroad cybersecurity literature by integrating a comprehensive overview of relevant studies and narrowing it down to the ones that address the above research questions.

2.1. SLR Workflow

Figure 1 illustrates the framework developed in this study for the SLR.

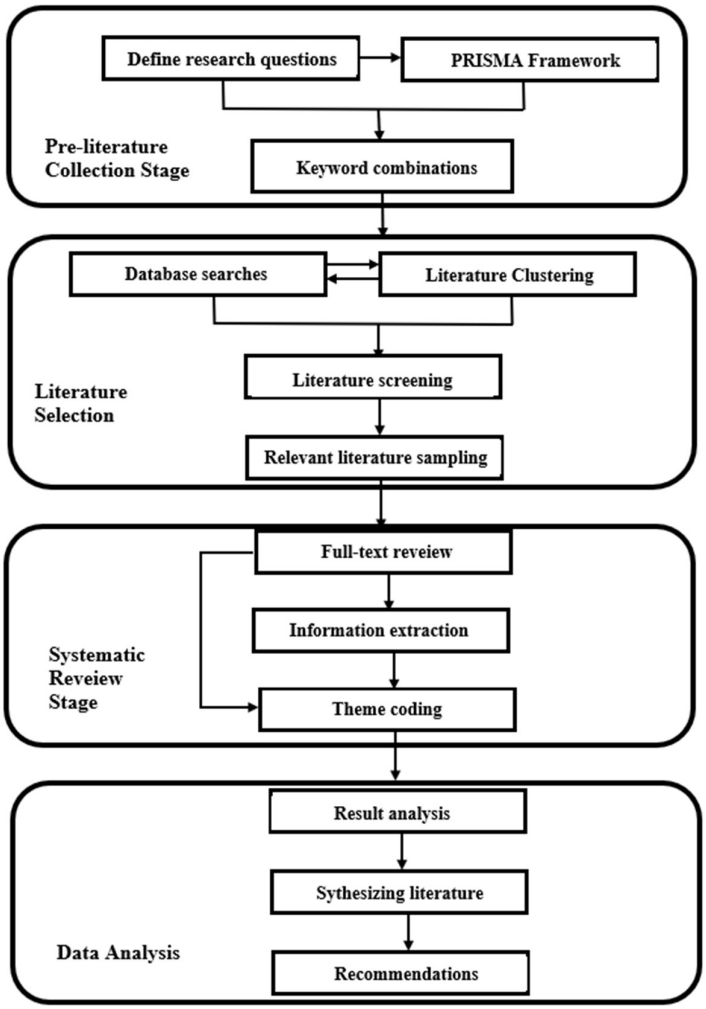

Figure 1. Framework of the study.

The main stages were as follows:

Pre-literature collection: Define the research questions, and their aim and scope. State the specific methodology or tools incorporated. This stage followed the PRISMA framework, which uses combinations of keywords and search phrases to produce potentially relevant results.

5. **Literature selection:** Conduct an electronic search of different databases using the defined search phrases that focus on the scope of the study. Screen the search results to eliminate irrelevant literature based on titles, abstracts, publication dates, language, keywords, and other criteria.47
6. **Systematic review:** Analyze the full text of relevant studies and classify the corpus based on the research questions and themes for further analysis.
7. **Data analysis:** Interpret the analysis by comparing and contrasting the literature analyzed.

 doi:10.20944/preprints202412.1013.v1

2.2. Pre-literature Collection Stage

This stage focused on identifying literature that addresses the four core research questions: challenges, protective measures, emerging trends, and innovations in cybersecurity within rail transportation. The research questions were critical in shaping the scope, emphasizing cybersecurity in the rail freight industry. The literature search included only journal and conference papers to ensure an elevated level of rigor.

Following the PRISMA framework, this stage carefully selected keywords and search phrases to target literature directly aligned with the study's scope. The search strategy aimed to encompass a broad range of relevant studies while systematically narrowing the results to those that best addressed the research questions. The authors then evaluated each identified source for its contribution to understanding the unique cybersecurity concerns in rail freight, as well as the industry's adaptation to emerging threats and technologies. This approach ensured a focused and comprehensive set of literature for the analysis, emphasizing both breadth and depth in addressing the complexities of rail freight cybersecurity.

2.3. Literature Selection

Guided by the research questions, the authors developed Boolean search commands to narrow the literature search and focus on relevant publications. The central premise for selecting relevant literature was to include scope for both rail freight transportation and the implementation of cybersecurity practices. Hence, the selected keywords and Boolean operators were ("rail freight" OR "railway security" OR "train transportation") AND ("cybersecurity" OR "cyberattacks" OR "cyber resilience" OR "cybersecurity practices"). The authors also considered regional variations of key words. For example, "train transportation" and "rail transportation" refer to the same scope reviewed in this study. The searches utilized the Google Scholar search engine and two databases: Web of Science and Science Direct. The authors selected these databases because they encompass a broad spectrum of interdisciplinary studies.

Table 1 summarizes the Boolean search commands and results from each tool. Search criteria included language, publication year, accessibility to text, uniqueness, and publication type. Table 2 summarizes the categories and criteria considered for the selected publications. The authors excluded reports that did not address the research questions.

2.4. Bibliometric Assessment

The bibliometric analysis assessed the temporal and geographic distribution of the selected body of literature to gain insights into the trends of discourse in railroad cybersecurity. The authors also utilized the NVivo software (version 14) [26] to categorize articles by analyzing their full text for relevance to the research questions, and to provide visualizations by a word cloud. The software provided a visualization of key terms, emphasizing gaps in extant studies. The authors also utilized the VOSviewer software (version 1.6.20) to visualize co-occurrence networks of important terms and concepts extracted from the selected body of literature [27]. The visualizations included term co-occurrence from the titles and abstracts to highlight the bibliographic coupling of key themes and concepts. Hence, the bibliographic networks provided a qualitative assessment and validation of the subject matter focus in the selected literature, highlighting the effectiveness of the SLR workflow and screening.

Table 1. Search results from the selected databases.

Database	Search Phrase and Format	Results
Google Scholar	("rail freight" OR "railway security" OR "train transportation") AND ("cybersecurity" OR "cyberattacks" OR "cyber resilience" OR "cybersecurity practices")	532

 doi:10.20944/preprints202412.1013.v1

Science Direct	("rail freight" OR "railway security" OR "train transportation") AND ("cybersecurity" OR "cyberattacks" OR "cyber resilience" OR "cybersecurity practices")	33
Web of Science	(TS=(rail freight transportation) OR TS=(railway security) OR TS=(train freight security)) AND (TS=(cybersecurity) OR TS=(cyberattacks) OR TS=(cyber resilience) OR TS=(cybersecurity practices))	4,658

Table 2. Criteria for relevant literature.

Category	Inclusion Criteria	Exclusion Criteria
Source type	Peer-reviewed journal articles and conference papers	Reports, dissertations, news, clinical trials, grants, etc.
Text accessibility	Full-text access to relevant publications	Availability of only title and/or abstract.
Language	English language	Not in English.
Search phrases	Based on the selected keywords	Keywords outside the chosen keywords.
Database	Relevant literature published in Google Scholar, Web of Science, and Science Direct	Published in other databases.
Uniqueness	Non-duplicate relevant studies from the selected databases	Duplicate publications from other databases or the selected databases.
Focus	Relevant studies focus on cybersecurity practices in the rail freight industry.	Studies outside the defined scope.
Publication date	January 2017 to November 2024	Studies published before January 2017 and after November 2024.

3. Results

The subsections that follow present the results of the literature screening, the bibliometric analysis to visualize and validate the screening results, and an assessment of the findings with respect to addressing the four research questions, and an evaluation of current industry practices.

3.1. Literature Screening

Figure 2 shows the results of the PRISMA workflow. The initial search yielded 5,223 studies across Google Scholar, Science Direct, and Web of Science. This result included peer-reviewed journal articles and conference papers from January 2017 to November 2024. To streamline the search for all the databases, the authors utilized the "refine function" for each database to limit the literature search to only journal and conference articles. Applying the inclusion and exclusion criteria in Table 2 reduced the relevant studies to 253 for further scrutiny. The initial screening phase identified and removed 2,251 duplicates and excluded an additional 2,701 studies that focused solely on either cybersecurity or rail freight transportation, without addressing both areas.

The authors removed an additional 18 studies because the abstracts and keywords did not align with the research area. Of the 253 articles screened, 99 studies lacked comprehensive data on cybersecurity framework in rail freight transportation, leaving 154 articles for further analysis. There were additional exclusions based on full text unavailability—some of the studies had only their abstracts in English with the full text in other languages, and some studies were not journal or conference papers. The final review yielded 70 articles.

 doi:10.20944/preprints202412.1013.v1

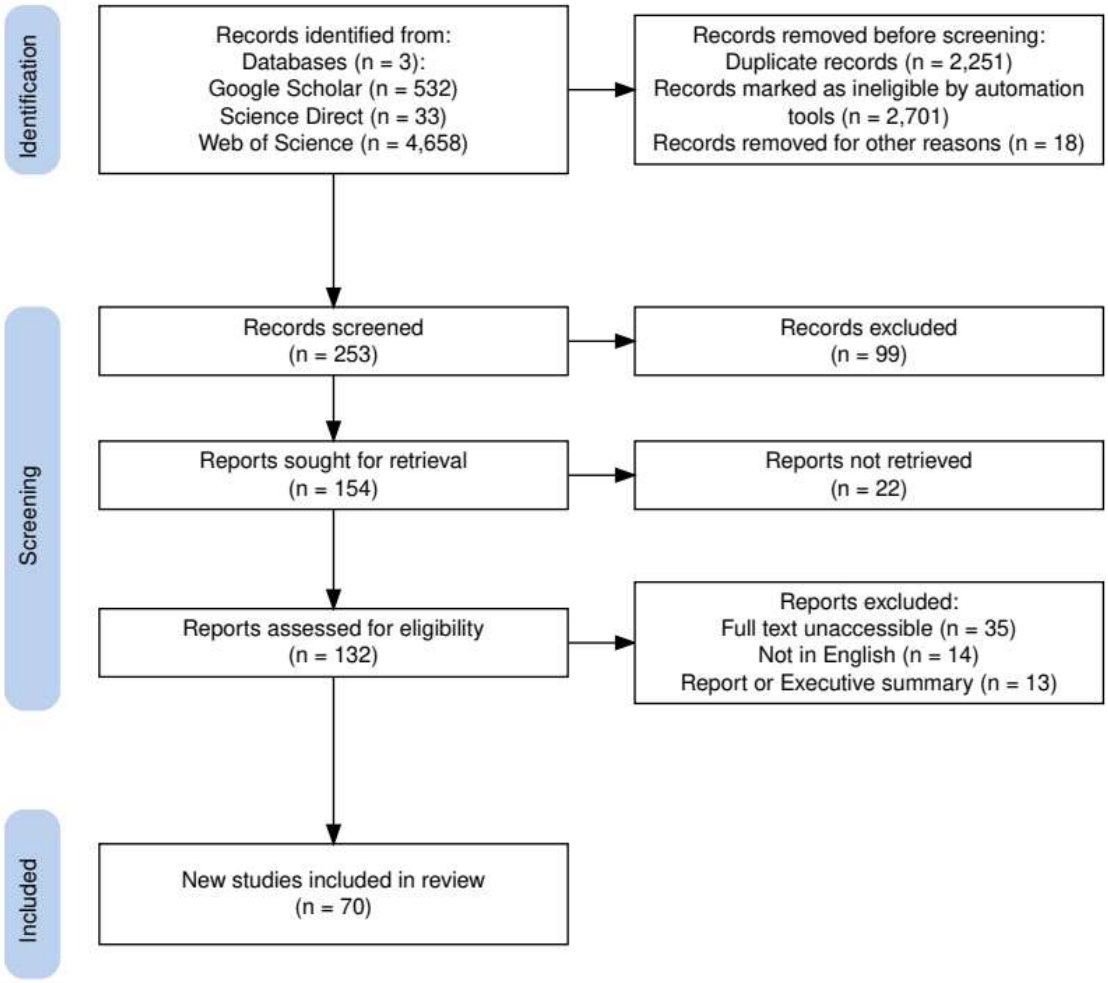

Figure 2. PRISMA workflow results.

3.2. Bibliometric Analysis

Figure 3 shows the temporal distribution of the publications. The number of publications steadily increased throughout the years, peaking in 2023. This reflects a growing trend in the integration of digital systems and autonomous operations in transportation, which has in turn increased vulnerability to cyber threats. Figure 4 shows the publication distributions by country. Sweden and France had the most publications on the topic, followed by Italy, the United States, and China. This reflects Sweden and France taking a lead role in railway cybersecurity research, stemming from Europe's continual investments in projects like Shift2Rail [14]. The Shift2Rail initiative is essential as it employs blockchain technology to ensure the security of data communication within rail systems. Nonetheless, the initiative does not adequately represent other regions like Africa and various areas in Asia, even as they increasingly embrace railroad infrastructure. This geographical disparity results in a significant oversight for these areas, largely attributed to limited resources, ineffective regulatory structures, or a deficit in understanding how to address intricate cybersecurity challenges within the railroad industry. In order to bridge this gap, there is a need for information that highlights a comprehensive approach to integrating technological innovation with operational strategies for effective policy implementations. Relevant studies highlighted in this study, therefore, aim to address advanced cybersecurity practices across diverse economies and infrastructure.

 doi:10.20944/preprints202412.1013.v1

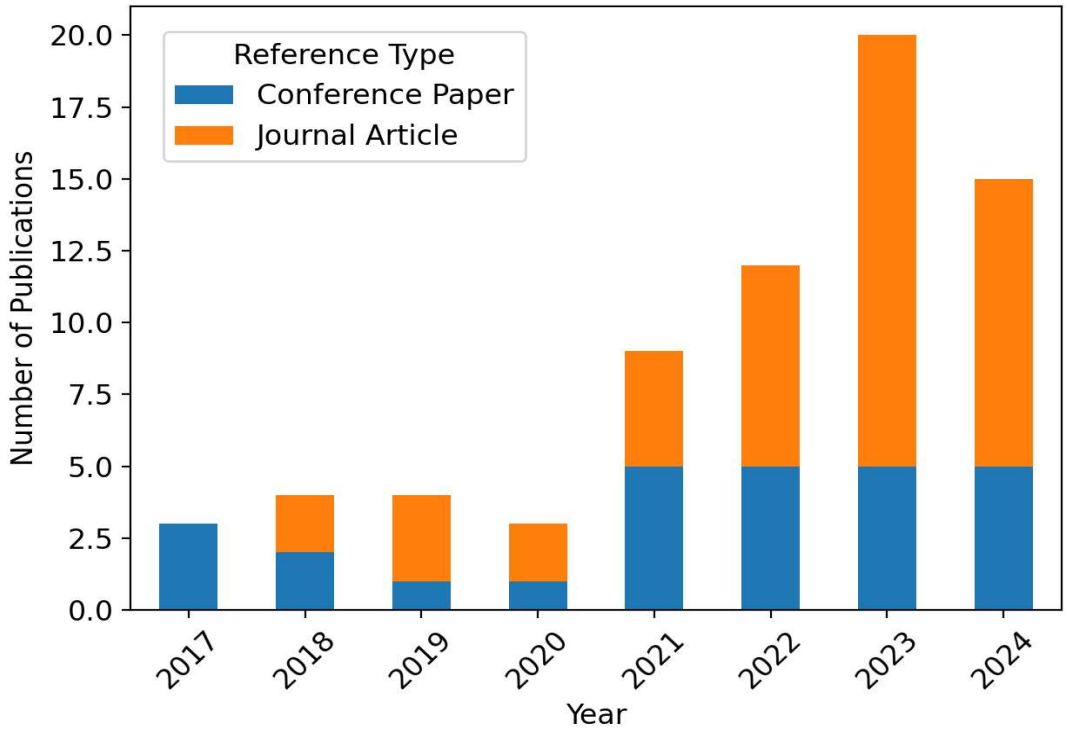

Figure 3. Distribution of publication by year and reference type.

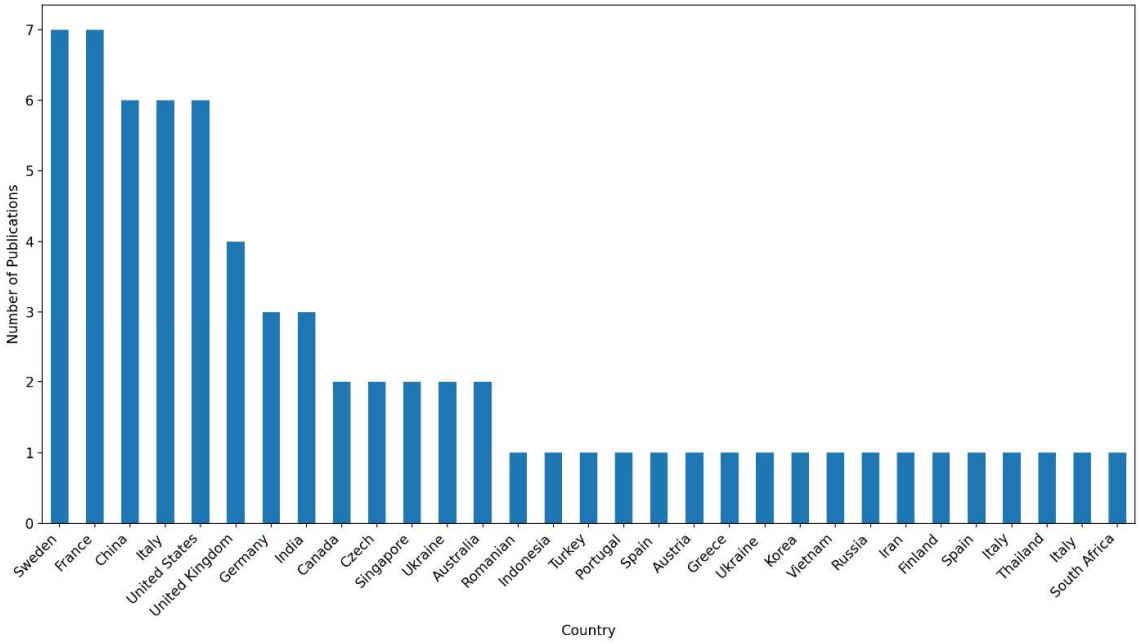

Figure 4. Number of publications by country.

Figure 5 shows a word cloud of the most frequently used terms in the selected corpus where the font size reflects their relative count. This word cloud validates the quality of the literature selection

 doi:10.20944/preprints202412.1013.v1

with the most frequent words being "railway," "train," "system," "safety," "attacks," "cybersecurity," and "security."

Figure 5. Word cloud for the relevant studies using NVivo.

Figure 6 shows the term co-occurrence network. The size of the circles represents the relative frequency of the term in the corpus. The thickness of the lines connecting terms represents the relative frequency of their co-occurrence in the corpus. The distinct colors represent cluster terms based on their co-occurrence and relationship within document subsets.

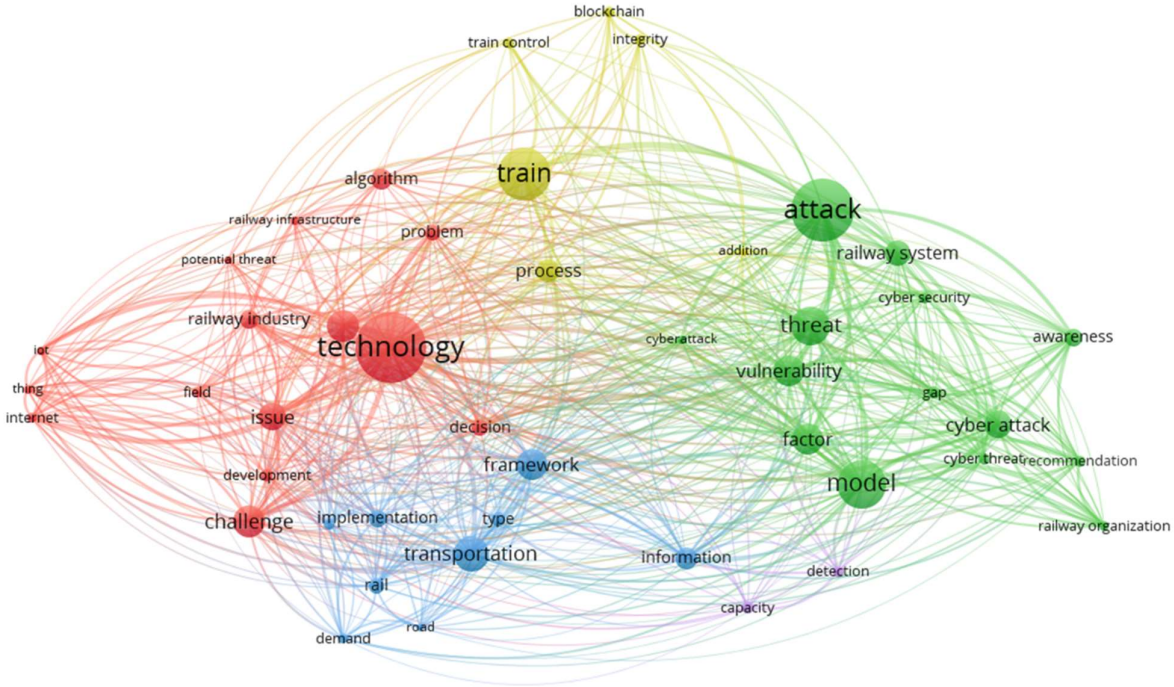

Figure 6. Term co-occurrence network.

These clusters represent thematic areas in the field. The largest cluster in red color, centered on "technology," emphasizes the pervasive role of technological advancements in addressing cybersecurity issues in rail freight systems. The other prominent cluster in green color focus on

 doi:10.20944/preprints202412.1013.v1

"threat," "attack," and "vulnerability," indicating concentrated research on vulnerabilities, cyberattacks, and operational impacts. Terms in the blue cluster like "transportation," "framework," and "implementation" reflect ongoing efforts to develop strategic and analytical approaches to mitigate risks in transportation systems. The connections among clusters demonstrate the interdisciplinary nature of cybersecurity, linking technological innovation with operational and strategic measures. This visualization highlights critical research areas and interdependencies, offering insights into emerging trends and gaps in the field. Table 3 classifies representative studies into the five categories and 12 themes shown.

Table 3. Categorization of the relevant studies.

Category	Category Explanation	Themes	References
Resilience and control systems	Studies that focus on resilient control systems for rail freight networks in terms of communication protocols and cyber monitoring systems	Control strategies	[28, 29, 17, 30, 31, 32]
		Autonomous monitoring	[28, 29, 33, 34, 16, 18, 35, 7, 2]
		Resilience framework	[36, 37, 38, 39, 40, 41, 42, 43]
Cryptographic mitigation and management	The application of cryptographic mitigation strategies for protecting data within the freight industry with the adoption of advanced encryption algorithms and frameworks	Data protection techniques	[44, 45, 46, 47, 48, 49, 50, 51, 52, 53]
		Encryption strategy	[54, 55, 56, 37, 57, 17, 58, 30]
Risk assessment	Identifying various rail freight cyber risks and assessing their impact on the sector through various risk assessment tools and evaluation metrics	Risk identification	[5, 34, 59, 19, 60, 61, 62, 63, 64]
		Risk evaluation	[43, 65, 51, 53, 55, 54]
		Risk impact	[16, 4, 31, 41, 49, 66]
Security frameworks	Includes studies that implement comprehensive frameworks for managing cyber threats within the rail industry by focusing on cybersecurity standards and policy frameworks	Cybersecurity standards	[36, 38, 40, 47, 50, 55, 67]
		Framework development	[68, 18, 17, 59, 69, 70]
Technology adoption	Explores the advancements in rail freight cybersecurity frameworks over the years in terms of technology adoption and deployment	Technology advancement	[40, 38, 41, 39, 71, 72]
		Practical implementations	[19, 36, 44, 73, 54, 56, 74, 75]

3.3. Types of Cyberattacks in the Rail Industry

There were 23 articles that focused on the types of cyberattacks common in the rail freight industry. The authors categorized them into five main types: anomaly detection, phishing, software vulnerability, malware, and denial of service, as shown in Table 4. Identifying the type of cyberattack is the first step in fully understanding the mitigation strategy to implement. All the studies asserted that these types of cyberattacks pose vulnerability to railroad operations. Even though various organizations have implemented numerous mitigation strategies, attackers often find other ways to disrupt operations [17]. Even though all these attacks increase vulnerability in the rail freight industry, their severity level differs [37].

 doi:10.20944/preprints202412.1013.v1

Table 4. Types of cyberattacks on rail freight transportation in the reviewed studies.

Attack Types	Description	Literature
Anomaly detection	Anomaly detection in cybersecurity involves recognizing patterns in a dataset that deviate from expected behavior. Identifying unauthorized access or malicious activity that differs from regular operations is crucial.	[5, 28, 33, 68, 80, 35]
Phishing page identification	Phishing is deceiving people into divulging confidential information, such as credit card numbers, usernames, and passwords, by seeming to be a reliable source in online correspondence. Phishing can also introduce malware into the network, which perpetrators can activate later to interfere with operations.	[35, 81, 17, 37, 55, 29, 79]
Software vulnerability diagnosis	This entails identifying and fixing software vulnerabilities that attackers could exploit to obtain unauthorized access or produce malicious results. Vulnerabilities can result in data breaches, impacting the confidentiality and integrity of critical business and operational data.	[28, 18]
Malware identification	Identifying malware entails detecting and eliminating malicious software programs created to damage or exploit any programmable device, service, or network. It is critical to identify and mitigate malware attacks to preserve the confidentiality and integrity of system data.	[28, 80, 17, 37]
Denial of Service (DoS)	Perpetrators design a denial-of-service attack to render a machine or network resource inaccessible to its intended users by temporarily or permanently disrupting the services of a host connected to the Internet. The rail freight industry must establish protocols to identify and address denial-of-service attacks to maintain rail freight transportation networks' uninterrupted and safe functioning.	[82, 5, 68, 17, 37]

Based on an analysis of 1,496 security breaches within a railway infrastructure from January to April 2021, the authors concluded that denial-of-service, phishing, and malware were the most frequent attack types, accounting for over 40% of incidents. Malware and denial-of-service attacks affected operational systems, leading to delays [76]. For instance, in 2016, the San Francisco rail system experienced a ransomware attack where passengers could ride for free [77]. In October 2017, a distributed denial of service (DDoS) attack targeted Sweden's transportation network, causing a system failure to track rail locations, which led to disruptions in road traffic maps [78]. These incidents underscore the importance of implementing layered defense strategies that include anomaly detection and training programs for employees to reduce these risks effectively. Phishing was by far the most common type of cyberattack in the rail freight industry [79], with five of the 23 papers discussing it. Such attacks involve sending deceptive emails to employees to gain unauthorized access to sensitive information within the business or sector. Some articles also highlighted other attack types, such as SQL injection, watering holes, cross-site scripting, malware, and brute force [17]. Despite phishing being the predominate type of attack in the railroad industry, affecting more of the recorded incidents in the sector [76], most of the suggested mitigation strategies focus on attack detection and network vulnerabilities rather than a layered strategy that combines

 doi:10.20944/preprints202412.1013.v1

real-time anomaly detection and awareness tailored to bridge the gap of human contribution to those risks. This disparity highlights a critical gap the study seeks to address.

3.4. Challenges of Cybersecurity in the Rail Industry

Research question 1 focused on different themes for the types of cyberattacks commonly reported in the rail freight industry, the vulnerability of the railway systems, and the risk assessment methodologies currently implemented to mitigate these challenges. The increase in automation across the transportation industry hinges on the reliance on digitalization and connectivity. While this initiative offers to increase efficiency and reduce cost, these systems become more vulnerable to cyberattacks. With the constant evolution of technology, the rail industry has evolved significantly from using coal-powered steam locomotives to integrating sophisticated technologies like PTC, reflecting significant technological advancements [1].

Seventeen of the relevant papers focused on network vulnerabilities in the rail freight industry. The studies asserted that the use of wireless communications makes these systems vulnerable to cyberattacks [82, 5, 28]. For example, Kiviharju et al. (2022) highlighted the need for an extensive evaluation of the communication systems in the European Rail Traffic Management System [5]. In addressing the issue of vulnerabilities in this industry, the authors identified three broad categories of vulnerabilities: (1) operational, (2) technical, and (3) interconnected. Table 5 characterizes the distinct types of vulnerabilities with their corresponding relevant studies. For example, while acknowledging the railway systems as a critical infrastructure in the transportation industry, Chan (2022) discussed the operational vulnerabilities within the sector [83]. On the other hand, Gaggero et al. (2024) highlighted the technical vulnerability within the industry, focusing on infrastructure attacks, especially the communication network [29]. The authors concluded by highlighting the gaps within the wireless communication industry. Soderi et al. (2023) highlighted that some of the vulnerabilities exist due to the industry's lack of a safety and security mindset during the manufacturing process [4]. Kour et al. (2020) highlighted the importance of becoming aware of attacks and vulnerabilities when evaluating cybersecurity programs in the rail freight industry [17].

Table 5. Types of vulnerabilities in the rail freight industry in the reviewed studies.

Vulnerabilities	Description	Relevant literature
Operational	This vulnerability stems from human errors, uncontrolled environmental conditions, or supply chain discrepancies that affect the rail freight industry's operations. Examples are incorrect data entry, miscommunication, rail freight supply chain failures, extreme weather conditions, and natural disasters.	[5, 28, 83, 84, 4, 85]
Technical	This vulnerability affects the rail freight industry's infrastructure and equipment. It includes derailments, mechanical failures, and aging technology, making the system more prone to failure and inefficiency.	[29, 34, 18, 35, 17]
Interconnected	Due to the complex nature of the rail freight network and its interconnectedness, a failure in one node might affect the entire system. These vulnerabilities may include data breaches, communication interruptions, and network intrusions. They may lead to data inaccuracy and system unreliability.	[82, 28, 68, 33]

Many relevant studies have presented steps for implementing risk assessment in the rail freight industry. Rekik et al. (2018) presented critical steps in assessing risks for train control and monitoring systems: (1) identification of critical assets, (2) assessing their vulnerabilities to cyberattacks, and (3) evaluating their likelihood and consequences of an attack [2]. The industry has also utilized tools like

 doi:10.20944/preprints202412.1013.v1

simulation and predictive models to assess potential cyberattack scenarios. For example, Kour et al. (2020) adopted the cyber kill chain model in a simulation scenario to assess potential cyberattacks [76]. The authors iterated the seven stages of this model developed by Lockheed Martin (2009), focusing more on the initial stages. Most studies asserted that the assessment should consider the cyber-physical nature of the constant evolution of technological advancements in rail freight systems to address the need for a cross-domain threat.

3.5. Risk Management in the Rail Industry

Research question 2 focused on existing cybersecurity measures in the rail freight industry through the lens of security frameworks and their components. The studies analyzed presented a broad range of mitigation methodologies for addressing risks in the rail freight industry. Each method presented a different approach to distinct types of cyberattacks. Each measure attempted to address an existing cyber security issue or to simulate a cyberattack. The authors delineated these measures into soft and hard strategies to reflect prevalent strategies implemented in the field. Soft strategies encompass measures that do not necessitate infrastructural changes but involve alterations in human training and operational methodologies within the rail freight industry. These strategies include training programs, adopting operational practices, and implementing regulations and standards. An example of a soft strategy is the new TSA regulation [11] implemented to help safeguard the transportation sector, including the railroad industry, against cyber-related disruptions. Conversely, hard strategies involve measures that require modifications to the physical infrastructure, such as upgrading security systems, enhancing network infrastructure, and implementing real-time monitoring systems and robust cyber-physical systems.

More than half of the studies suggested a soft strategy approach to address various rail freight industry risks. A significant body of literature highlighted the importance of continuous employee training as a cornerstone of cybersecurity. Thaduri et al. (2019) highlighted the shift toward digitalization in the rail freight industry [7]. They hinted at various soft strategies such as human factor training, policy development and compliance, information sharing and collaboration, incident response and management, and continuous auditing to protect sensitive information within the railway freight industry. Thron et al. (2024) recommended a dynamic strategy for educating employees on cybersecurity [36]. Rekik et al. (2018) implied undertaking a comprehensive threat landscape assessment like the one proposed in the ROLL2RAIL project to determine unmitigated cyber risks [2]. The other half of the studies adopted the hard strategies approach. The most common strategy was an improved firewall and intrusion detection system, which is essential for early detection within the systems [82, 83, 28]. Overall, the rail freight industry can enhance its defenses against cyberattacks by conducting cyber-physical security risk assessments and implementing customized security measures.

3.6. Emerging Trends in the Rail Freight Industry

This section focuses on research question 3 to explore trends in network security management and future directions in rail cybersecurity. This industry is evolving rapidly by integrating modern technologies and methods to improve safety and cybersecurity. For example, electric-powered trains are emerging to establish greener, more energy-efficient rail freight systems [86]. Enhancing cybersecurity awareness and providing training is crucial for increasing the reliability and robustness of railway systems, emphasizing the beneficial influence of a cybersecurity culture in businesses [17]. The emergence of Industry 4.0 has also assisted in the convergence of information technology in the railway industry, resulting in reliability and operational efficiency [57]. The evolution of technology in the rail freight industry has warranted constant reliance on communication systems for signaling, thereby creating growing concerns due to system vulnerabilities [87]. Therefore, in ensuring rail freight transportation safety, there should be comprehensive traffic management within the networks in addition to infrastructure management [88]. Another emerging technology is the use of blockchains to provide a decentralized security framework in managing transactions, improving reliability and data distribution across various networks and components [45]. Adopting a zero-trust

 doi:10.20944/preprints202412.1013.v1

architecture (ZTA) is another emerging model in the rail freight industry to ensure strict access and continuous authentication to minimize inside threats and cyberattacks [89]. There has been a significant shift toward predictive strategies where systems are proactive to threats and provide mitigation strategies based on patterns and modern technology [17]. Overall, the future of rail freight transportation should incorporate sustainable practices and advanced technologies while simultaneously adopting relevant cybersecurity measures.

3.7. Current Practices in the Rail Freight Industry

This section explores research question 4 in terms of the extent that current cybersecurity practices mitigate cyberattack risks in rail transportation and research gaps. As a recurring theme, the reviewed studies described the constant evolution of technology as a significant contributing factor to cyber vulnerability in the rail freight industry. For example, Kour et al. (2019) asserted that the increased vulnerability of railroads to cyberattacks stems from the integration of advanced technologies during maintenance processes [57]. Falahati and Shafiee (2022) discussed the use of machine learning algorithms and fuzzy logic systems in detecting and responding to cyberattacks in rail freight transportation [60]. Likewise, Singh et al. (2021) highlighted the implementation of advanced cybersecurity measures in autonomous rail operations to safeguard communication systems and operational data [30]. Thaduri et al. (2019) shed light on the importance of comprehensive training programs as a risk mitigation tool [7].

4. Discussion

The subsections that follow link the original research questions to the themes exposed in the results for a comprehensive understanding of cybersecurity in the rail freight industry.

4.1. Assessment of Rail Freight Mitigation Strategies

Numerous studies argued that due to the constant evolution of technology within the railway industry, a continuous and adaptive cyber mitigation strategy is essential. This suggests the need to cross-integrate some cyber assessment strategies from other sectors to tackle the issue within the railway industry. Stakeholders within the railway industry must explore benchmark practices within adjacent industries such as aviation and connected vehicles using vehicle-to-anything communications and adapt their strategies. This adoption becomes especially crucial with a greater reliance on automation, control, and communications technology to improve safety and security. Using a robust quantitative approach such as predictive models for multi-stage cyberattack simulation can be effective [76]. Another key strategy is cybersecurity awareness and training. Railroads can cultivate a cyber hygiene culture [32], especially where employees maintain the security and integrity of digital systems and data [90]. This practice has been in the healthcare sector and other areas, and it has been beneficial in safeguarding sensitive electronic information [91, 92]. Additionally, stakeholders within the railway sector should leverage technologies such as blockchains to enhance the security and integrity of their transactions [93].

4.2. Technological Adaptation in the Rail Industry

It is evident that technological evolution is crucial in streamlining processes in the rail industry. These technological solutions will require continuous human improvement and education, organizational measures and methodologies, and improved digitalization with advanced networks. Human improvement should emphasize dynamic, scenario-based programs that replicate real-world issues, promoting a proactive cybersecurity culture within the workforce. The rail freight industry has begun adopting a ZTA to build a reliable system that combats ambiguous security boundaries within a complex network. For instance, Feng et al. (2023) proposed a theoretical use of blockchains and the Merkle tree [89]. ZTA has demonstrated its effectiveness in implementing stringent authentication measures and restricting unauthorized access to a network by continuously verifying access requests. However, the practical implementation of this approach may result in significant

 doi:10.20944/preprints202412.1013.v1

challenges, including regulatory compliance, human factors, inherent security concerns, and interoperability. To effectively implement ZTA, the industry must develop targeted strategies to minimize potential risks. There will be a need for constant skills development, hands-on training, and real-life experiences through optimal training delivery methods. This research highlights the need to expand the use of the ZTA to more effectively align with predictive models, including AI-based real-time threat assessment and blockchain-supported decentralized data exchange. These improvements would bolster the resilience of rail systems, especially in tackling emerging threats within interconnected networks.

4.3. Mitigating Cybersecurity Gaps in Rail Freight

This section highlights plausible recommendations to fill strategic gaps within the rail freight industry regarding cybersecurity. A permanent solution in cybersecurity is impossible because threats continuously evolve. Hence, implementing fewer targeted strategies to enhance cybersecurity measures may improve efficiencies. In addressing the issue of human errors, the deployment of autonomous trains could be a significant step in improving safety in the rail industry [30]. However, this also comes with a significant risk as autonomous systems possess different vulnerabilities within the rail network due to their interconnectedness for real-time information access. This may require advanced encrypted techniques to mitigate potential threats. Combining advanced technological strategies and taking a proactive organizational approach can significantly enhance the industry's resilience against cyber threats.

4.4. Enhancing Cybersecurity Resilience in Rail Freight

Existing works on cybersecurity in the rail freight industry have focused on balancing operating efficiency and incorporating advanced technology. This review highlights the significance of maintaining a robust security framework to accommodate technological changes that avoid operation disruptions [35, 83, 60, 29]. The theoretical work of Thron et al. (2024) highlighted the balance between human factors and cybersecurity risks [36]. The study highlighted that many industries, including the aviation sector, also face similar challenges in balancing automation and human error [94]. In particular, ongoing human resource training and development initiatives are necessary to reduce human error, which is a severe cybersecurity vulnerability. Furthermore, utilizing advanced technology for threat detection and response, such as machine learning and artificial intelligence, can aid in addressing changing cybersecurity issues [60]. Current research indicates that collaboration and information sharing among stakeholders significantly improves cybersecurity in the rail industry [93]. International cooperation and public-private partnerships can enhance the exchange of threat intelligence and best practices.

While soft strategies like human training may provide a more economical approach, their potential for scalability and long-term effectiveness has yet to be evaluated. On the other hand, hard strategies, such as firewalls and anomaly detection systems, tackle technical risks but do not provide solutions for mitigating human-centric threats like phishing. The railroad industry needs to learn from related sectors that emphasize the use of predictive analytics. For optimal effectiveness, blockchain-enabled decentralized data sharing should support these frameworks to improve resilience across interconnected networks while responding to ongoing technological advancements.

Recommendations for Policymakers

Improving cybersecurity measures in the railroad sector demands specific approaches that involve all parties, including policymakers and industry practitioners. They are essential in developing the regulatory framework and securing the funding to tackle various issues, such as cyber threats. As a result, governance must implement compulsory cybersecurity regulations while ensuring that current policies are adhered to. Frameworks such as ISO 27001 or NIST should be adopted in countries with a limited understanding of railroad cybersecurity. This will help maintain

 doi:10.20944/preprints202412.1013.v1

consistency among operators and ensure adherence to international best practices [18, 49]. As mentioned earlier, incorporating Zero Trust Architecture (ZTA) [89, 60] is essential for improving overall authentication and access management while reducing the likelihood of security breaches.

Public-private partnership between rail operators, cybersecurity firms, and academicians can foster innovation. The Shift2Rail initiative [14, 40] serves as a successful example of how collaboration can effectively tackle cybersecurity issues in the railway sector, demonstrating its ability to address vulnerabilities within rail systems. In order for all the proposed strategies to be successful, policymakers must also budget for innovation in this area. Innovative technologies like AI-driven predictive analytics [76] and blockchain data structures [45] have demonstrated effectiveness in tackling cybersecurity issues, so it is essential to allocate specific funds for their implementation.

The authors accounted for both scalability and collaboration to guarantee the effective execution of these recommendations. The strategies proposed in this study are flexible for rail operators of different sizes and they are also combinable with other models to tackle the challenge of interoperability. Given that the railroad industry consists of interconnected systems, many of the proposed strategies and recommendations are relevant for achieving unified global standards and minimizing regional disparities.

5. Conclusions

This work summarized the research on cybersecurity practices in the rail freight industry by focusing on the growing literature published in peer-reviewed journals and conference papers. To focus the review, the authors posed four research questions within the following categories: (1) challenges, (2) measures, (3) emerging trends, and (4) cybersecurity practices. The study collated findings from 70 relevant peer-reviewed articles and conference papers. In addressing the first research question, the study highlighted that technological evolution and human error significantly impact cybersecurity practices. Technological evolution in the rail freight industry revolves around the increasing utilization of advanced digital systems to improve operational efficiency and safety. On the other hand, the literature attributes human error to insufficient training, a lack of situational awareness, and the complexities of managing recent technologies.

The review identified common threats such as anomaly detection, phishing, software vulnerabilities, malware, and denial-of-service categorized into operational, technical, and interconnectedness vulnerabilities. The second research question focused on measures implemented to enhance cybersecurity, differentiating between hard strategies, which involve physical infrastructure changes, and soft strategies focusing on operational and training adjustments. The third research question addressed emerging trends, including automation, zero-trust architecture, blockchain, and machine learning, highlighting concerns over system vulnerabilities due to technological advancements. The research emphasized current cybersecurity practices and their effectiveness in risk reduction.

The authors identified obstacles and recommendations for future research, including the need for standardized cybersecurity protocols, investment in human resources, and stakeholder collaboration for sharing best practices and threat intelligence. Despite these strategies, uncertainty remains about whether specific strategies will effectively address ongoing cybersecurity challenges in the rail freight industry and how to best coordinate these strategies with technological functions.

Despite these developments, research must fill substantial gaps. For example, there is a need for additional investigation into integrating cybersecurity measures with existing operational technology and information technology systems while maintaining seamless functionality. Additionally, establishing a unified defense mechanism necessitates the development of standardized cybersecurity protocols specifically designed to meet the unique requirements of the rail industry.

This study also emphasized the importance of taking a proactive and unified approach to cybersecurity in the railroad sector, highlighting the need to address technical and human-related vulnerabilities. The swift development of technology and changing industry trends present substantial opportunities and challenges for cybersecurity within the rail freight industry. This

 doi:10.20944/preprints202412.1013.v1

research highlights various potential areas for future investigation that aim to fill existing gaps in the literature and prepare for anticipated emerging threats. Future research should aim to create adaptable frameworks that blend AI-powered predictive tools, which are gradually becoming the foundation of cybersecurity mitigation strategies across industries, with established cybersecurity standards, especially in regions often underrepresented. Policymakers and industry stakeholders should make these initiatives a priority to protect global rail systems from emerging cyber threats, ensuring the safety of critical supply chains, and promoting sustainable development around the world.

Funding: This research received funding from the United States Department of Transportation, Center for Transformative Infrastructure Preservation and Sustainability (CTIPS), Funding Number 69A3552348308.

Data Availability Statement: This article includes the data presented in the study.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. U.S. DOT, "PTC Communications: Cybersecurity Technology Review and Concept of Operations," Washington, 2023.
2. M. Rekik, C. Gransart and M. Berbineau, "Cyber-physical Threats and Vulnerabilities Analysis for Train Control and Monitoring Systems," in 2018 International Symposium on Networks, Computers and Communications (ISNCC), Rome, 2018.
3. S. Soderi, D. Masti and Y. Z. Lun, "Railway cyber-security in the era of interconnected systems: a survey," IEEE Transactions on Intelligent Transportation Systems, 2023.
4. S. Soderi, D. Masti, M. Hämäläinen and J. Iinatti, "Cybersecurity Considerations for Communication Based Train Control," IEEE Access, vol. 11, pp. 92312-92321, 4 2023.
5. M. Kiviharju, C. Lassfolk, S. Rikkonen and H. Kari, "A Cryptographic and Key Management Glance at Cybersecurity Challenges of the Future European Railway System," 2022.
6. A. Woodburn, "Rail network resilience and operational responsiveness during unplanned disruption: A rail freight case study," Journal of Transport Geography, vol. 77, no. 1, pp. 59-69, 2019.
7. A. Thaduri, M. Aljumaili, R. Kour and R. Karim, "Cybersecurity for eMaintenance in railway infrastructure: risks and consequences," International Journal of System Assurance Engineering and Management , vol. 10, p. 149–159, 2019.
8. P. Singh, Z. Elmi, V. K. Meriga, J. Pasha and M. A. Dulebenets, "Internet of Things for sustainable railway transportation: Past, present, and future," Cleaner Logistics and Supply Chain, vol. 4, 2022.
9. Z. Wang and X. Liu, "Cyber security of railway cyber-physical system (CPS) – A risk management methodology," Communications in Transportation Research, vol. 2, 2022.
10. P. López-Aguilar, E. Batista, A. Martínez-Ballesté and A. Solanas, "Information Security and Privacy in Railway Transportation: A Systematic Review," Sensors 22, vol. 22, no. 20, 2022.
11. Freight Waves, "TSA proposes new cybersecurity rule for some railroads, other transit systems," 07 11 2024. [Online]. Available: https://www.freightwaves.com/news/tsa-proposes-new-cybersecurity-rule-for-some-railroads-other-transit-systems. [Accessed 12 11 2024].
12. The Record , 24 September 2024. [Online]. Available: https://therecord.media/railroad-cyberthreats-tsa-regulations. [Accessed 13 November 2024].
13. A. Newton, "Multimodal transport security: frameworks and policy applications in freight and passenger transport," Security Journal, vol. 30, no. 1, pp. 328-330, 2017.
14. É. Masson and C. Gransart, "Cyber security for railways-a huge challenge-Shift2Rail perspective," in International Workshop on Communication Technologies for Vehicles, Cham, 2017.
15. THALES, "Cybersecurity for Rail," 18 October 2019. [Online]. Available: https://www.thalesgroup.com/en/worldwide/transport/news/cybersecurity-rail. [Accessed 8 February 2024].
16. J. Prochazka, P. Novobilsky, D. Prochazkova and T. Kertis, "Certification Cycles of Train Cyber Gateway," in Proceedings of the 29th European Safety and Reliability Conference (ESREL), 2020.
17. R. Kour, R. Karim and A. Thaduri, "Cybersecurity for railways – A maturity model," Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, vol. 234, no. 10, pp. 1129-1148, 4 2020.
18. E. Bellini, S. Marrone and F. Marulli, "Cyber Resilience Meta-Modelling: The Railway Communication Case Study," Electronics, vol. 10, no. 5, p. 583, 4 2021.
19. J. Szyliowicz and L. Zamparini, "Freight transport security and the robustness of global supply chains," Transport Reviews, vol. 42, no. 6, pp. 717-724, 2022.

20. N. Demiridis and C. Pyrgidis, "Getting freight trains back on track–How railway undertakings, infrastructure owners and regulators can navigate the main dilemmas in freight business to drive sustainable growth," Frontiers in Sustainability, vol. 3, 2022.
21. S. Aminzadegan, M. Shahriari, F. Mehranfar and B. Abramović, "Factors affecting the emission of pollutants in different types of transportation: A literature review," Energy Reports, vol. 8, pp. 2508-2529, 2022.
22. A. Jain, R. v. d. Heijden, V. Marchau and D. Bruckmann., "Towards Rail-Road Online Exchange Platforms in EU-Freight Transportation Markets: An Analysis of Matching Supply and Demand in Multimodal Services," Sustainability, vol. 12, no. 24, 2020.
23. M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, R. Chou, J. Glanville, J. M. Grimshaw and A. Hróbjartsson, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," International Journal of Surgery, vol. 88, 2021.
24. D. Tranfield, D. Denver and P. Smart, "Towards a methodology for developing evidence-informed management knowledge by means of systematic review," British Journal of Management, vol. 14, no. 3, pp. 207-222, 2003.
25. M. J. Grant and A. Booth, "A typology of reviews: an analysis of 14 review types and associated methodologies," Health information & libraries journal, vol. 26, no. 2, pp. 91-108, 2009.
26. NVivo, QSR International, 2024. [Online]. Available: https://lumivero.com/product/nvivo/.
27. N. J. v. Eck and L. Waltman, "VOSviewer," Leiden University, 1 July 2024. [Online]. Available: vosviewer.com. [Accessed 30 June 2024].
28. N. Miller, Y. Satsrisakul, K. Faist, M. Fehling-Kaschek, S. Crabbe, M. Poliotti, N. Naderpajouh, S. Setunge, S. Ergün, A. Kanak, S. Tanrıseven, A. Lekidis, E. Matsika, P. Sick and E. Cazzato, "A Risk and Resilience Assessment Approach for Railway Networks," 2021.
29. G. B. Gaggero, M. Marchese and P. Girdinio, "A survey on wireless-communication vulnerabilities of ERTMS in the railway sector," Journal of Surveillance, Security and Safety, vol. 5, no. 1, pp. 52-61, 2024.
30. P. Singh, M. A. Dulebenets, J. Pasha, E. D. R. S. Gonzalez, Y.-Y. Lau and R. Kampmann, "Deployment of Autonomous Trains in Rail Transportation: Current Trends and Existing Challenges," IEEE Access, vol. 9, pp. 91427-91461, 4 2021.
31. A. Fakhereldine, M. Zulkernine and D. Murdock, "Detecting Intrusions in Communication-Based Train Control Systems," in ICC 2022 - IEEE International Conference on Communications, Seoul, 2022.
32. O. Bal, "Formation and management of safety culture in the railway industry: best practices and strategies," Collection of Scientific Works of the State University of Infrastructure and Technologies Series "Transport Systems and Technologies", pp. 69-80, 2023.
33. G. Sharma, E. Sherif, M. He and E. Boiten, "Analysis of Cyber-Attacks for Modern Digital Railway System Using Cyber Range," 2022.
34. S.-H. Xiong, M.-R. Qiu, G. Li, H. Zhang and Z.-S. Chen, "Balancing the signals: Bayesian equilibrium selection for high-speed railway sensor defense," Information Sciences, 2024.
35. S. Abdellaoui, E. Dumitrescu, C. Escudero and E. Zamaï, "Cyber Threat Assessment in Monitoring Turnout Railway Systems," 2023.
36. E. Thron, S. Faily, H. Dogan and M. Fr, "Human factors and cyber-security risks on the railway – the critical role played by signalling operations," Information and Computer, vol. 32, no. 2, pp. 236-263, 2024 .
37. A. N. Nebaba, I. K. Savvas, M. A. Butakova, A. V. Chernov and P. S. Shevchuk, "Improving Multiclass Classification of Cybersecurity Breaches in Railway Infrastructure using Imbalanced Learning," ESSE 2021: 2021 2nd European Symposium on Software Engineering, pp. 100-105, 4 2021.
38. A. T. Hoang and X. K. Nguyen, "Managing Technological Security of Smart Environment Monitoring Systems: Study Of a coastal province in Vietnam," International Journal of Critical Infrastructures, vol. 19, no. 4, pp. 383-403, 2023.
39. J. Prochazka, P. Novobilsky and D. Procházková, "Mobile Cyber Gateway Security Control," in Proceedings of the 31st European Safety and Reliability Conference, 2021.
40. D. Varvarigou, D. Espes and G. Bersano, "Orchestrator for ensuring interdependency between safety and cybersecurity in railway control systems," International Journal of Rail Transportation, vol. 12, no. 4, pp. 1-16, 2023.
41. Z. Wang, X. Hei, W. Ma, Y. Wang, K. Wang and Q. Jia, "Parallel anomaly detection algorithm for cybersecurity on the highspeed train control system," Mathematical Biosciences and Engineering, pp. 287-308, 2022.
42. G. Bearfield, C. V. Gulijk and R. J. Thomas, "Redefining rail systems verification and validation: The safety/security STAIRCASE model," Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, vol. 237, no. 2, pp. 266-274, 2023.

43. X. Ge, Q. Wu, Q.-L. Han and X.-M. Zhang, "Resilient Virtual Coupling Control of Automatic Train Convoys with Intermittent Communications," IEEE Transactions on Vehicular Technology, pp. 1-12, 2023.
44. G. A. Weaver, "Scientific Data Management for Interconnected Critical Infrastructure Systems," in 2021 ACM/IEEE Joint Conference on Digital Libraries (JCDL), Champaign, 2021.
45. S. Kim and D. Kim, "Securing the Cyber Resilience of a Blockchain-Based Railroad Non-Stop Customs Clearance System," Sensor, vol. 23, no. 6, 2023.
46. Y. Purwanto, M. F. Ruriawan, A. Alamsyah, F. P. Wijaya, D. N. Husna, A. Kridan, F. N. A. Fakhrudin, M. Itqon, M. Y. Febrianta, S. Widiyanesti, F. Mentari and A. A, "Security Architecture for Secure Train Control and Monitoring System," Sensors, vol. 23, no. 3, 2023.
47. G. Hatzivasilis, K. Fysarakis, S. Ioannidis, I. Hatzakis, G. Vardakis, N. Papadakis and G. Spanoudakis, "SPD-Safe: Secure Administration of Railway Intelligent Transportation Systems," Electronics, vol. 10, no. 1, 2021.
48. S. Backman and M. Rhinard, "The European Union's capacities for managing crises," Journal of Contingencies and Crisis Management, vol. 26, no. 2, pp. 261-271, 2018.
49. C. Schmittner, P. Tummeltshammer, D. Hofbauer, A. M. Shaaban, M. Meidlinger, M. Tauber, A. Bonitz, R. Hametner and M. Brandstetter, "Threat Modeling in the Railway Domain," in Reliability, Safety, and Security of Railway Systems, 2019.
50. V. Romero and E. B. Fernández, "Towards a Security Reference Architecture for Cyber- Physical Systems," in The 15th LACCEI International Multi-Conference for Engineering, Education, and Technology: "Global Partnership for Development and Engineering Education, 2017.
51. S. Marrone, "Towards a Unified Definition of Cyber and Physical Vulnerability in Critical Infrastructures," in 2017 IEEE European Symposium on Security and Privacy: Workshops (EuroS&PW), Paris, 2017.
52. I. Babeshko, O. Illiashenko and F. D. Giandomenico, "Towards Effective Safety and Cybersecurity Co-engineering in Critical Domains," in 2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), Athens, 2023.
53. S. R. Aktouche, M. Sallak, A. Bouabdallah and W. Schön, "Towards Reconciling Safety and Security Risk Analysis Processes in Railway Remote Driving," in 2021 5th International Conference on System Reliability and Safety (ICSRS), Palermo, Palermo, Italy, 2021.
54. I. Agirre, A. J. Calderon, I. Yarza, I. Mugarza, D. Garcia and L. Borracci, "UP2DATE software updating framework compliance with safety and security regulations and standards," in 2023 26th Euromicro Conference on Digital System Design (DSD), Golem, Albania, 2023.
55. A. R. Yekta, D. Spychalski, E. Yekta, C. Yekta and S. Katzenbeisser, "VATT&EK: Formalization of Cyber Attacks on Intelligent Transport Systems - a TTP based approach for Automotive and Rail," CSCS '23: Computer Science in Cars Symposium, pp. 1-17, 4 2023.
56. Q. Wang, W. Yu, D. Huang and Y. Guo, "Weighted Train-to-Train Communication-Based Data-Driven Consensus Tracking of Multiple HSTs Subject to Deception Attacks," IEEE Transactions on Vehicular Technology, vol. 73, no. 5, pp. 6346-6356, 2023.
57. R. Kour, M. Al-Jumaili, R. Karim and P. Tretten4, "eMaintenance in railways: Issues and challenges in cybersecurity," Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, vol. 233, no. 10, pp. 1012-1022, 2019.
58. R. Kour and R. Karim, "Cybersecurity workforce in railway: its maturity and awareness," Journal of Quality in Maintenance Engineering, vol. 27, no. 3, pp. 453-464, 2021.
59. S. Chakrabarty and B. Sikdar, "Detection of Cyber Attacks on Railway Autotransformer Traction Power Systems," IEEE Transactions on Industry Applications, vol. 59, no. 6, pp. 7188-7200, 2023.
60. A. Falahati and E. Shafiee, "Improve Safety and Security of Intelligent Railway Transportation System Based on Balise Using Machine Learning Algorithm and Fuzzy System," International Journal of Intelligent Transportation Systems Research, vol. 20, no. 1, pp. 117-131, 4 2022.
61. J. Nunes, T. Cruz and P. Simões, "Railway Infrastructure Cybersecurity: An Overview," in Proceedings of the 23rd European Conference on Cyber Warfare and Security, 2024.
62. S. Abdellaoui, E. Dumitrescu, C. Escudero and E. Zamaï, "Temporal assessment of malicious behaviors: application to turnout field data monitoring," in International Conference on Control, Automation and Diagnosis (ICCAD24), Paris, France, 2024.
63. I. Avcı and M. Koca, "A Novel Security Risk Analysis Using the AHP Method in Smart Railway Systems," Applied Sciences, vol. 14, no. 10, 2024.
64. B. v. Niekerk, "Vulnerability of South African Commodity Value Chains to Cyber Incidents," Scientia Militaria: South African Journal of Military Studies, vol. 51, no. 3, pp. 161-186, 2023.
65. T. Zoppi, I. Mungiello, A. Ceccarelli, A. Cirillo, L. Sarti, L. Esposito, G. Scaglione, S. Repetto and A. Bondavalli, "Safe Maintenance of Railways using COTS Mobile Devices: The Remote Worker Dashboard," ACM Transactions on Cyber-Physical Systems, vol. 7, no. 4, pp. 1-20, 2023.

66. X. Ge, Q.-L. Han and X.-M. Zhang, "Secure virtual coupling control of connected train platoons under cyber attacks," Vehicle System Dynamics, pp. 1-28, 2024.
67. S. G. Predescu, D. Savu and V. E. Badea, "Cybersecurity in the Railway Sector," Romanian Cyber Security Journal, vol. 4, no. 2, 2022.
68. A. Fakhereldine, M. Zulkernine and D. Murdock, "CBTCset: A Reference Dataset for Detecting Misbehavior Attacks in CBTC Networks," Florence, 2023.
69. M. H. ter Beek, A. Fantechi, S. Gnesi, G. Lenzini and M. Petrocchi, "Can AI Help with the Formalization of Railway Cybersecurity Requirements?," in International Symposium on Leveraging Applications of Formal Methods, 2024.
70. I. Voronko, "The security of IoT systems in railway transport," Transport Systems and Technologies, vol. 43, 2024.
71. K. Vayadande, A. Bhoyar, A. Gorave, H. Behare, Y. Bhale and O. Bhojane, "Secure Stations: Revolutionizing Railway Security Using AI," in International Conference on Innovations and Advances in Cognitive Systems, 2024.
72. S. Janani, S. Vijayaram and R. C. Vijayganesh, "IoT-SafeRails: Revolutionizing Railway Collision Avoidance Technology," 2024 International Conference on Inventive Computation Technologies (ICICT), pp. 1666-1673, 2024.
73. M. Heinrich, J. Vieten, T. Arul and S. Katzenbeisser, "Security Analysis of the RaSTA Safety Protocol," in 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, Florida, 2018.
74. M. Dai, G. Li and W. Du, "Research on data sharing and exchange technology in the railway industry based on blockchain," in 7th International Conference on Traffic Engineering and Transportation System (ICTETS 2023), 2024.
75. P. Kongsap and S. Kaewunruen, "Agent-based modelling of high-speed railway interdependent critical infrastructures facing physical and cyber threats," Frontiers in Built Environment, 2024.
76. R. Kour, A. Thaduri and R. Karim, "Predictive model for multistage cyber-attack simulation," International Journal of System Assurance Engineering and Management, vol. 11, no. 3, pp. 600-613, 3 2020.
77. MIT Technology Review, "Ransomware Took San Francisco's Public Transit for a Ride," MIT Technology Review , 28 November 2016. [Online]. Available: https://www.technologyreview.com/2016/11/28/69496/ransomware-took-san-franciscos-public-transit-for-a-ride/. [Accessed 1 December 2024].
78. B. Barth, "DDoS attacks delay trains, stymie transportation services in Sweden," SC Media , 13 October 2017. [Online]. Available: https://www.scworld.com/news/ddos-attacks-delay-trains-stymie-transportation-services-in-sweden. [Accessed 1 December 2024].
79. O. Osliak, A. Saracino, F. Martinelli and P. Mori, "Cyber threat intelligence for critical infrastructure security," Concurrency and Computation Practice and Experience, vol. 35, no. 23, 2023.
80. B. Zou, P. Choobchian and J. Rozenberg, "Cyber resilience of autonomous mobility systems: cyber-attacks and resilience-enhancing strategies," 2021.
81. P. Ungkap and T. Daengsi, "Cybersecurity Awareness Modeling Associated with Influential Factors Using AHP Technique: A Case of Railway Organizations in Thailand," 2022.
82. B. Gao, B. Bu and X. Wang, "A Comprehensive Resilient Control Strategy for CBTC Systems Through Train-to-Train Communications Under Malicious Attacks," IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 11, pp. 21015-21033, 4 2022.
83. R. Chan, "A Security Framework for Railway System Deployments," Cham, 2022.
84. S. Rahiminia, A. Mehrabi, M. Pourseyed Aghaee and A. Jamili, "Adopting a Bi-level Optimization Method for the Freight Transportation Problem: A Multi-objective Programming Approach," Transportation Research Record: Journal of the Transportation Research Board, vol. 2677, no. 2, pp. 490-504, 4 2023.
85. L. J. Valdivia, I. Adin, S. Arrizabalaga, J. Anorga and J. Mendizabal, "Cybersecurity-The Forgotten Issue in Railways: Security Can Be Woven into Safety Designs," IEEE Vehicular Technology Magazine, vol. 13, no. 1, pp. 48-55, 2018.
86. A. A. Merchan, S. Belboom and A. Léonard, "Life cycle assessment of rail freight transport in Belgium," Clean Technologies and Environmental Policy, vol. 22, p. 1109–1131, 2020.
87. H. Steele, C. Roberts and S. Hillmansen, "Railway smart grids: Drivers, benefits and challenges," Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, vol. 233, no. 5, pp. 526-536, 2019.
88. J. Kanis, A. D. and M. Kmetik, "Draft of strategy of the European rail freight corridor Amber," in MATEC Web of Conferences , 2018.

 doi:10.20944/preprints202412.1013.v1

89. Y. Feng, Z. Zhong, X. Sun, L. Wang, Y. Lu and Y. Zhu, "Blockchain enabled zero trust based authentication scheme for railway communication networks," Journal of Cloud Computing, vol. 12, no. 62, 2023.
90. R. Kour, A. Thaduri and R. Karim, "Railway Defender Kill Chain to Predict and Detect Cyber-Attacks," Journal of Cyber Security and Mobility, vol. 9, no. 1, p. 47–90, 2019.
91. S. Nifakos, K. Chandramouli, C. K. Nikolaou, P. Papachristou, S. Koch, E. Panaousis and S. Bonacina, "Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review," Sensors, vol. 21, no. 15, p. 5119, 2021.
92. R. Alkhaledi and S. Hawamdeh, "Electronic Health Records and Cyber Hygiene: A Qualitative Study of the Awareness, Knowledge, and Experience of Physicians in Kuwait," Proceedings of the Association for Information Science and Technology, vol. 60, no. 1, 2023.
93. C. Laiton-Bonadiez, J. W. Branch-Bedoya, J. Zapata-Cortes, E. Paipa-Sanabria and M. Arango-Serna, "Industry 4.0 Technologies Applied to the Rail Transportation Industry: A Systematic Review," Sensors, vol. 22, no. 7, p. 2491, 2022.
94. A. T. Miranda, "Understanding Human Error in Naval Aviation Mishaps," Human Factors, vol. 60, no. 6, pp. 763-777, 2018.