IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 18 June 2024, accepted 11 July 2024, date of publication 29 July 2024, date of current version 13 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3434618

RESEARCH ARTICLE

Ensuring the Integrity, Confidentiality, and Availability of IoT Data in Industry 5.0: A Systematic Mapping Study

KERSON BOISROND[1], PIERRE MARTIN TARDIF[1], AND FEHMI JAAFAR[2]
[1]Computer Science Department, University of Sherbrooke, Sherbrooke, QC J1K 2R1, Canada
[2]Computer Science and Mathematics Department, University of Quebec at Chicoutimi, Chicoutimi, QC G7H 2B1, Canada

Corresponding authors: Kerson Boisrond (kerson.boisrond@usherbrooke.ca), Pierre Martin Tardif (pierre-martin.tardif@usherbrooke.ca), and Fehmi Jaafar (fehmi.jaafar@uqac.ca)

This work was supported by the Contributions of NSERC's Discovery Program and Public Safety Canada's Cyber Security Cooperation Program.

ABSTRACT The significant success of the Internet of Things in facilitating connections among consumer devices has led to an evident inclination towards connecting devices within industrial environments, commonly known as the Industrial Internet of Things (IIoT). Meanwhile, the integration of DevOps and DevSecOps into Industry 5.0 is generating much interest in both industry and academia, and its adoption in practice is raising a lot of challenges. This study aims to organize the knowledge about the challenges encountered by the Industry and practitioners when adopting DevOps and DevSecOps in the Industry 5.0 environment, as well as suggested practices documented in the literature. We also identify the security challenges related to data integrity, confidentiality, and availability of Industrial IoT data. We conducted a Systematic Mapping Review of more than a thousand papers and focused on 57 peer-reviewed studies published between January 2019 and March 2024. We have identified challenges and benefits associated with adopting DevOps and DevSecOps in Industry 5.0. We have also identified specific security solutions, particularly in the Industrial Internet of Things (IIoT), as well as the correlation between these findings. The study results were classified into organizational, technical, and regulatory. The findings show that the most frequently reported challenges and solutions were related to technical. Although organizational factors were considered critical for successfully adopting DevOps and DevSecOps in Industry 5.0, they required more investigation. Our study offers a comprehensive analysis of the research to secure the industrial Internet of Things, discusses their applicability, and analyzes their security benefits by integrating DevOps and DevSecOps in Industry 5.0.

INDEX TERMS DevOps, secure DevOps, DevSecOps, industry 5.0, Industrial Internet of Things (IIoT), Internet of Things (IoT), continuous integration, continuous deployment, continuous delivery, integrity, confidentiality, availability, artificial intelligence, cyber security.

I. INTRODUCTION

We are currently experiencing a significant change towards the fifth industrial revolution, driven by digitization. DevOps is a methodology that facilitates the integration between software development (Dev) and its operational deployment (Ops), emphasizing the automation of the entire process. References [31], [33], [47], and [80]. However, with the growing need for secure software applications, a new field called DevSecOps has emerged, which incorporates security practices into the DevOps process. DevSecOps has been implemented successfully in traditional software development systems. However, the challenges of the industrial environment require the adaptation of DevSecOps frameworks that meet the standards of Industry 5.0 [9], [16]. To improve the

The associate editor coordinating the review of this manuscript and approving it for publication was Amjad Mehmood.

development process and minimize security risks, it is essential to integrate continuous risk assessment into the development cycle. This helps eliminate any hindrances between development and operations and reduces vulnerabilities. Developing and ensuring the quality of Industry 5.0 systems requires adopting continuous engineering practices, which include ongoing planning, integration, and deployment [7], [31]. In today's world, ensuring the security of data in the Industrial Internet of Things has become a considerable challenge. With the disclosure of more and more vulnerabilities, attackers are becoming increasingly sophisticated in their attacks. They go beyond encrypting data using ransomware malware and engage in data theft, unauthorized disclosures, and intrusions. They use the stolen data in any possible way to harm the affected business. At present, there are no established methods in software engineering to prove compliance with security standards while implementing DevOps and DevSecOps practices in Industry 5.0. For software to be considered secure, it must safeguard its data and code, ensuring that confidentiality, integrity, and availability are not compromised. Security is an essential component of the software development life cycle, and its proper implementation allows for the full utilization of DevOps. This paper presents a systematic mapping of the literature on using DevOps and DevSecOps pipelines in Industry 5.0 research over the past decade. The review sheds light on the topic and highlights the challenges that need to be addressed before implementing DevOps and DevSecOps on Industry 5.0 and a large scale in highly regulated industries with stringent quality standards, particularly concerning security.

We researched to assess the current state of DevOps adoption and security DevOps in Industry 5.0. To do this, we analyzed more than a thousand papers and focused on 57 primary studies from various online libraries.

The contribution of this paper is outlined based on the information gathered from the literature. This particular systemic mapping focuses on DevOps-based security solutions for Industry 5.0, particularly in IIoT systems.

The paper begins by presenting a background of DevOps and DevSecOps, industry 5.0, Industrial IoT systems, and other related themes. It also delves into the topic of the benefits and challenges when applying DevOps, DevSecOps in Industry 5.0. Additionally, the systematic mapping highlights security in Industrial IoT, discussing potential attacks and their effects on each layer. Furthermore, a comprehensive review of possible security solutions for IIoT is provided, presented by DevSecOps and considering published papers until 2024.

This document is structured as follows: Section II explains the basic principles of DevOps and DevSecOps in Industry 5.0. Section III outlines the design, while Section IV presents the results. Finally, Section V discusses our perspective and the potential implications for researchers and practitioners.

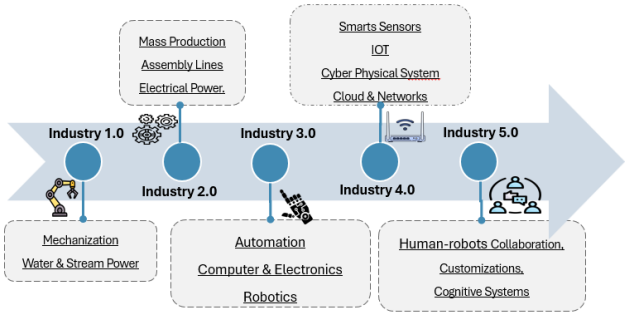

FIGURE 1. Evolution of the industrial revolutions.

II. BACKGROUND

In this section, we provide background information on DevOps and DevSecOps, as well as other similar terms, as outlined in our systematic mapping.

A. INDUSTRY 4.0

There have been several industrial revolutions that have brought about significant changes in manufacturing methods. Figure 1 shows the evolution of the industrial revolution. The first industrial revolution was characterized by mechanization, while the second saw the introduction of mass production, automation, and electrification. Industry 3.0 incorporated IT and automation [11]. Industry 4.0 refers to the fourth industrial revolution. It is the integration of advanced technologies, such as the Internet of Things (IoT), artificial intelligence (AI), robotics, and big data analytics, into manufacturing processes. Roblek et al. [71], described Industry 4.0 as a concept introduced in Germany that is revolutionizing the manufacturing and service sectors through cyber-physical systems and the IoT. The primary aim is to establish ''smart factories'' that are remarkably automated, versatile, and productive. These factories can adjust to dynamic customer requirements and market conditions in real-time. Industry 4.0 involves the real-time supervision and management of machinery and equipment in all phases of the production process. Industry 4.0 [11], aims to increase the value of manufacturing operations regardless of labor costs. The main objective is to optimize the manufacturing process by making the equipment as versatile as possible and creating flexible production lines that can run continuously without downtime.

Industry 5.0: The Industry 5.0 paradigm refers to a new approach to industrial processes that combines smart manufacturing with advanced Machine Learning (ML) applications. This paradigm aims to revolutionize industrial processes by incorporating ML technologies and enabling collaboration between humans and machines [32]. Trstenjak et al. [83] describe the concept of Industry 5.0 which aims to promote symbiotic collaboration between human and machine activities. This concept intends to ensure the well-being and sustainability of industrial workers. The emergence of Industry 5.0 is due to the challenges and

resistance faced during the implementation of Industry 4.0, which includes concerns related to social justice and sustainability.

B. ARTIFICIAL INTELLIGENCE

Artificial Intelligence (AI) is a diverse field of study that aims to develop computer systems capable of simulating human intelligence in various ways. It combines concepts from mathematics, cognitive science, computational neurobiology, and mathematical logic to create machines that can perform intelligent tasks. AI can be used to solve problems, make decisions, comprehend natural language, understand the environment, learn from data, and much more. It is utilized in many fields, such as robotics, computer vision, natural language processing, and machine learning. AI is constantly evolving and has a wide range of applications, particularly in the fields of medicine, finance, transport, and industry. Machine learning (ML), a type of AI, is based on algorithms that enable systems to learn and improve iteratively based on the data they process.

ML has developed rapidly in the past decade and has been adopted in almost every field of business and research. It has shown superior results compared to traditional software applications in many areas, such as medical diagnostics. It has even outperformed humans in tasks that typically require human intelligence [45].

1) MACHINE LEARNING (ML) APPLICATIONS

Machine Learning applications refer to the use of algorithms and statistical models to enable computers to learn and make predictions or decisions without being explicitly programmed. In the context of Industry 5.0, ML applications are used to analyze large amounts of data generated by industrial processes and make intelligent decisions or predictions to optimize operations [25].

It is a relatively new field that focuses on improving and optimizing the entire lifecycle of machine learning models. This includes all stages, from the initial development of the models to their deployment and ongoing maintenance [41]. The goal of MLOps is to streamline and make processes more efficient in working with machine learning models. This is important because the development and deployment of ML models can be complex and time-consuming, involving various steps such as data preprocessing, model training, evaluation, and deployment [40]. By implementing MLOps practices, organizations can ensure that their ML models are developed and deployed more systematically and efficiently. This can lead to faster development cycles, improved model performance, and easier maintenance and updates. MLOps involves the use of various tools, technologies, and best practices to automate and standardize the processes involved in ML models. This includes version control systems for tracking changes to models and data, continuous integration and delivery (CI/CD) pipelines for automating the deployment process, and monitoring and logging systems for tracking model performance and detecting issues [40].

C. DEVOPS

DevOps is a software development culture that allows organizations to deliver high-quality software products using process automation efficiently [3]. In this approach, software development, quality assurance, and operations teams work together in an agile model to deliver software continuously. This helps to speed up the deployment process and reduces the time required to integrate user feedback. DevOps practices aim to automate the deployment process by creating automated environments, which reduces the need for manual handovers between the development and operations teams in the world of software development. Continuous integration and continuous delivery (CI/CD) pipelines are crucial components of the DevOps approach. These pipelines are designed to automate the various stages of the software development life cycle (SDLC), including code building, acceptance testing, and deployment to storage and production environments. By aligning different processes and tools, DevOps teams can streamline their workflow and ensure that their software development practices are efficient and effective. Ultimately, the pipeline produces artifacts that can be used to demonstrate compliance [54]. Having a deployment pipeline is crucial in software development because it monitors changes made to the software from version control to the end-user. Automating this process simplifies the deployment process for software developers who may require direct access to development and production environments [45]. Normally, infrastructure teams are responsible for handling the deployment pipeline. DevOps identifies three major software security risks: sacrificing security for speed and agility, treating security as an afterthought, and environmental risks.

Devops Pratices:

- *Continuous integration (CI):* Continuous Integration is a widely adopted DevOps practice that involves automatic building, testing, and validation of code changes. It ensures that code changes are thoroughly tested and validated, providing quick feedback to developers. By identifying defects early in the development process, product quality is improved. Integration can be challenging if not performed promptly. Automatic building and testing of code are initiated when commits are made to a shared repository [17], [94].
- *Continuous Delivery (CD):* Continuous delivery is a practice in software development that involves the automatic delivery of software sprints after code testing. It builds on continuous integration and enables developers to release and deploy software at any time, thereby speeding up the process of obtaining customer feedback. In essence, continuous delivery is a technique that facilitates the quick and efficient release of software [94].
- *Continuous Deployment (CD):* Continuous deployment is an advanced version of Continuous Delivery that allows software output to be automatically deployed to a production environment, provided that they meet all

the necessary quality gates. It is a push-based method that deploys software changes to production through the deployment pipeline without the need for human intervention [66], [67].

- *Infrastructure as Code:* IaC encompasses the management and provisioning of infrastructure through the utilization of coding and automated processes [66], [67]. The inclusion of security controls within the infrastructure code guarantees that security becomes an intrinsic component of the deployment procedure for the infrastructure.
- *Containerization and Orchestration:* Containerization enhances deployment flexibility, while orchestration tools like Kubernetes play a pivotal role in managing containerized applications across various domains, from cloud to automotive networks and edge computing scenarios. Containerization such as Docker and orchestration platforms such as Kubernetes, are often utilized in DevSecOps to achieve scalable deployment. To ensure the security of containerized applications and orchestration environments, various security measures are implemented [66], [67].

D. DevSecOps

DevSecOps is a methodology that brings together the development (Dev), security (Sec), and delivery/operations (Ops) of software systems. This approach aims to reduce the time between software requirement and delivery while maintaining high software security through continuous integration and continuous delivery (CI/CD) [66], [67]. DevSecOps ensures that security measures are integrated into a DevOps environment by promoting collaboration between development, operations, and security teams. To ensure compliance with DevOps security standards, it is important to have a clear understanding of how to strategically incorporate security requirements into DevOps pipelines [54].

Developers usually concentrate on writing and updating code, while operations personnel are responsible for managing and maintaining systems. Security is a persistent process that needs to be applied in every phase and then comprehensively throughout the whole system. The complexity of the security increases as the number of interfaces grows, which can be challenging to handle [50].

E. INTERNET OF THINGS

The Internet of Things (IoT) refers to the connection of digital devices to the physical environment through IT systems, which allows communication between them. Its use is becoming more widespread, especially in the automotive, telecommunications, and healthcare sectors. IoT presents new prospects in industries such as energy management, preventive maintenance, and production line automation [11]. These are devices, such as sensors, appliances, and machines, that leverage the Internet of Things (IoT) connectivity to improve industrial and manufacturing processes. There are various applications of IoT, such as home automation, smart buildings, smart cities, medicine, and self-driving cars. IoT has specific applications in industry for energy management, preventive maintenance, and automation [11]. The research opportunity involves exploring security and privacy solutions for the Internet of Things within the scope of DevOps in Industry 4.0. The IoT is vulnerable to cyber threats, so it is vital to develop effective methods that can protect data and detect intrusions.

Industrial Internet of Things (IIoT): In the industrial context, the IIoT offers opportunities for energy management, preventive maintenance, and automation. The IIoT refers to the use of IoT technologies in industrial and machine-to-machine (M2M) communication fields. It is used mainly in smart factories or automation settings [11]. IIoT is a subdomain of Industry 5.0, which integrates the IoT concept into smart manufacturing. In other words, IIoT is the network of intelligent and highly connected industrial components that are deployed to achieve high production rates with reduced operational costs through real-time monitoring, efficient management, and controlling of industrial processes, assets, and operational time.

F. DATA SECURITY

Confidentiality, integrity and availability (CIA) are the three key elements of information security. They refer to the fundamental security controls in an information system, which traditionally focused on technical measures to protect those aspects of information [86].

- ***Integrity:*** A crucial aspect of maintaining integrity is to ensure that data are kept in their current form and are not subject to unauthorized manipulation. Essentially, this means that both external and insider threats should be prevented from modifying the data [37].
  DevSecOps highlights the significance of maintaining the integrity of data and code. It ensures that data and code remain accurate and unchanged throughout the development and deployment process. This is accomplished through various practices such as version control, code reviews, and automated testing to identify and prevent unauthorized changes.
- ***Confidentiality:*** Confidentiality ensures that unauthorized persons or parties cannot access the information and data either from within or outside the system. Encryption algorithms are used to maintain the confidentiality of data and information during storage and transmission, and access to data locations is reduced to enhance security. Ensuring data is kept private and accessible only to authorized [37]
  DevSecOps aims to protect sensitive information from unauthorized access. It employs access controls, encryption, and secure data handling practices to maintain the confidentiality of data. This is crucial to safeguarding user data and business secrets.

- ***Availability:*** Availability refers to the ability of a system to provide services and produce products on time. It ensures that all subsystems are functioning correctly and are capable of working on time as needed. This guarantees the proper functioning of all industrial systems and prevents failures such as hardware and software corruption, power outages, and DoS attacks. It is also important for device users (or the devices themselves) to have access to the services they need whenever they need them. To achieve this, different software and hardware components must be robust enough to provide services even in the presence of malicious entities or adverse situations. Ensuring that systems and data are accessible when needed [37] DevSecOps ensures availability and performance by preventing downtime due to security incidents through measures such as redundancy, load balancing, and disaster recovery planning.

III. STUDY DESIGN

For this systematic mapping study, we used the modified snowball method as outlined by Claes Wohlin [92] to collect our articles. Our study design includes details on our search keywords, technique, data sources, and criteria for inclusion and exclusion.

A. RESEARCH QUESTIONS AND MOTIVATION

We strive to identify pertinent publications regarding the development and utilization of DevOps and DevesecOps in the context of Industry 5.0. These publications address the concerns of Industry 5.0 through the application of DevOps and DevSecOps techniques. Furthermore, we explore the publications in which their contributions are published, and the timeframe in which these contributions were made. This inquiry is encapsulated in the following set of research questions.

While conducting a systematic mapping review following the guidelines of Keele et al. [36] and Petersen et al. [63], we refer to a list of research questions and motivations as a guide. The following questions and motivations are:

RQ1: What are the research trends of DevOps in Industry 5.0?

The motivation is to discover the published scientific research level and explore where academics share their findings on implementing DevOps in Industry 5.0 applications. Gain insight into the types of contributions made over the years.

RQ2: What are the benefits of the adoption of DevOps in Industry 5.0?

To see the benefits of incorporating DevOps practice in Industry 4.0.

RQ3: What are the challenges of implementing DevOps in Industry 5.0?

This query identifies organizations' challenges when adopting DevOps, as highlighted in the existing literature.

RQ4: What is the Current Adoption of DevOps and DevSecOps in Industry 5.0?

In the literature, we are curious about the solutions, specific guidelines, best practices, tools, frameworks, or technologies. Previous DevSecOps studies or surveys have not yet explored this area thoroughly.

RQ5: What are the DevSecOps tools or applications that provide security and safety in Industry 5.0?

Our goal is to pinpoint any gaps that the research community identifies based on the answers to Questions 1 and 2.

RQ6:How DevSecOps can ensure the confidentiality, availability, and integrity of data in industry 5.0

To see how DevSecOps can ensure the confidentiality, availability, and integrity of data in industry 5.0, and more specifically in the industrial Internet of Things.

B. SELECTION PROCESS

To conduct our study, we followed a four-step process. Figure 2 shows the stages of research and the selection of studies. First, we chose digital repositories commonly used in systematic literature reviews (SLRs) focused on software engineering, including Springer Link, Science Direct, ACM, Scopus, and IEEE Xplore. Next, we create search strings and perform an initial search to retrieve the first set of primary documents from these repositories. Finally, we performed an exhaustive search using the search strings to select the main studies. To define search criteria, follow these tree steps: 1. Use research questions to establish key terms. 2. Identify synonyms and alternative spellings for each main term. 3. Verify the search terms in titles, abstracts, and keywords.

We used the following search string following the steps outlined above:

("Devops" ***OR*** *"DevSecOps"* ***OR*** *"SecDevOps"* ***OR*** *"Secure DevOps"* ***OR*** *"Continuous Integration"* ***OR*** *"Continuous Delivery"* ***OR*** *"Continuous Deployment")* ***AND*** *("Industry 5.0"* ***OR*** *"Industrial production"* ***OR*** *"manufacturing system"* ***OR*** *"IoT"* ***OR*** *"Industrial Internet of Things"* ***OR*** *"IIoT")*

We used these search strings to collect all articles from the above digital libraries.

1) SELECTION CRITERIA

To include work that supports research questions, we defined selection criteria based on the title, abstract, and presence of keywords in the search string within the content.

Inclusion criteria: We have selected potentially pertinent documents by applying the subsequent three criteria:

1) Studies that have undergone rigorous evaluation by experts in the field and have been published in reputable academic sources such as journals, conferences, and workshops.
2) Research can be conveniently accessed through electronic means.

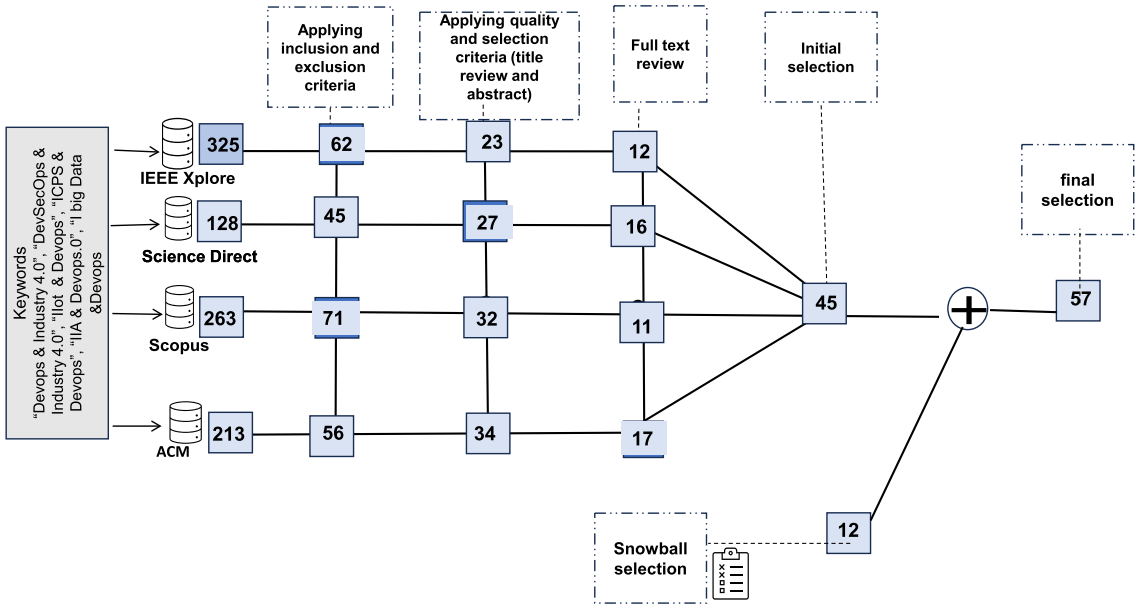

FIGURE 2. The stages of research and selection of primary studies.

3) Based on the title, abstract, and keywords, it can be concluded that the paper primarily addresses the development or utilization of DevOps or DevSecOps in the context of Industry 5.0.

Exclusion Criteria: Documents that meet the inclusion criteria but are excluded based on the following criteria:

1) Studies not available in English.
2) Studies lacking systematic peer review, such as books, slides, and websites.
3) Brief papers and teasers, measuring less than two pages, that include calls for papers, editorials, or curricula.
4) Study that the full text is not available.

2) DATA EXTRACTION

In order to gather information from the primary studies that were identified, we created a template which is detailed in Table 1. Each field in the template includes a data item and a corresponding value. The data extraction process was reviewed by the second and third authors, who double-checked the accuracy of the information collected from each paper.

As of January 17, 2024, we've gathered 1149 initial studies from five digital repositories using the search string. We excluded certain studies based on title, abstract, and keywords, leaving us with 217 primary studies. These primary studies underwent thorough screening using inclusion and exclusion criteria, and finally, we narrowed them down to 57 studies, as shows Figure 2.

The table below shows the data sources and search outcomes.

TABLE 1. Study extraction form.

Study item	Description	RQ
Study ID	Integer	
Article Title	name of the article	
Author name	The full name of the authors	
Year	Publication year of the study.	
Venue	The name of the publishing venue.	RQ1
Authors affiliation	Academia or industry or both.	RQ1
Publication type	Journal, conference, workshop, book	RQ1
Benefits	The Benefits reported in the study related to the adoption of DevOps or DevSecOps in industry 5.0	RQ2
Challenges	The Challenges reported in the study related to the adoption of DevOps or DevSecOps in industry 5.0	RQ3
Tools	The strategies reported in the study related to the adoption of DevOps or DevSecOps in industry 5.0	RQ4
Tools	The Tools reported in the related study used in DevOps or DevSecOps in industry 5.0	RQ5
Security	The security strategy reported in the study related to DevOps or DevSecOps in industry 5.0	RQ6

IV. RESULTS

The publications selected were carefully examined to answer the research questions raised. We pay attention to (1) the trend of the evolution of all the research studies and the different places where they have been published; (2) the researchers' focus on applying DevOps to Industry 5.0; (3) the benefits, challenges, adoption, and prioritization of backlogse use of DevOps and DevSecOps in IoT in Industry 5.0.

TABLE 2. Selected primary studies.

List of selected publications			
ID	Ref	Title	Year
P01	[23]	Self-Service Cybersecurity Monitoring as Enabler for DevSecOps	2019
P02	[26]	Towards Model-Based Continuous Deployment of Secure IoT Systems	2019
P03	[31]	Industrial DevOps	2019
P04	[2]	Integrating Security with DevSecOps: Techniques and challenges	2019
P05	[79]	DevOps in Industry 4.0: A Systematic Mapping	2019
P06	[24]	DevOps Transformation for Multi-Cloud IoT Applications	2019
P07	[47]	An Empirical Taxonomy of DevOps in Practice	2020
P08	[55]	Integration of Security Standards in DevOps Pipelines: An Industry Case Study	2020
P09	[70]	Continuous Security Testing: A Case Study on Integrating Dynamic Security Testing Tools in CI/CD Pipelines	2020
P10	[84]	A Software Architecture for the Industrial Internet of Things—A Conceptual Model	2020
P11	[52]	Guide to Implementing DevSecOps for a System of Systems in Highly Regulated Environments	2020
P12	[49]	Preliminary Findings about DevSecOps from Grey Literature	2020
P13	[20]	Methods of implementation, Maturity Models and definition of Roles in DevOps frameworks: A systematic Mapping -	2020
P14	[56]	Remote and agile improvement of industrial control and safety systems processes	2020
P15	[43]	IoT-based Systems Actuation Conflicts Management Towards DevOps: A Systematic Mapping Study	2020
P16	[53]	Security impacts of sub-optimal DevSecOps implementations in a highly regulated environment.	2020
P17	[44]	DevOps in an ISO 13485 Regulated Environment: A Multivocal Literature Review	2020
P18	[75]	On the Role of Software Architecture in DevOps Transformation: An Industrial Case Study	2020
P19	[9]	Monitoring Real Time Security Attacks for IoT Systems Using DevSecOps: A Systematic Literature Review	2021
P20	[21]	Blockchained Adaptive Federated Auto MetaLearning BigData and DevOps CyberSecurity Architecture in Industry 4.0	2021
P21	[85]	Software Architecture of a Fog Computing Node for Industrial Internet of Things	2021
P22	[62]	Understanding the context of IoT software systems in DevOps	2021
P23	[42]	Adoption of DevOps Practices in the Finnish Software Industry: an Empirical Study	2021
P24	[50]	DevSecOps in Robotics	2021
P25	[51]	Integrating multi-disciplinary offline and online engineering in industrial cyber-physical systems through DevOps	2021
P26	[61]	A systematic review on the use of DevOps in internet of things software systems	2021
P27	[33]	The Titan Control Center for Industrial DevOps analytics research	2021
P28	[72]	Towards a Secure DevOps Approach for Cyber-Physical Systems: An Industrial Perspective	2021
P29	[48]	Industrial Internet of Things and its Applications in Industry 4.0: State of The Art	2021
P30	[69]	Holding on to Compliance While Adopting DevSecOps: An SLR	2021
P31	[59]	DevSecOps Methodology for the NG-IOT Ecosystem Development Lifecycle ASSIST-IOT PERSPECTIVE	2021
P32	[18]	MAP: Design, Development, Deployment, and Maintenance of Industry 4.0 AI Applications	2022
P33	[10]	Challenges of Adopting DevOps Culture on the Internet of Things Applications - A Solution Model	2022
P34	[66]	Challenges and solutions when adopting DevSecOps: A systematic review	2022
P35	[89]	Using a Semantic Knowledge Base to Improve the Management of Security Reports in Industrial DevOps Projects	2022
P36	[27]	Prevalence of continuous integration failures in industrial systems with hardware-in-the-loop testing	2022
P37	[19]	Controlled Continuous Deployment: A Case Study From The Telecommunications Domain	2022
P38	[68]	A DevSecOps-enabled Framework for Risk Management of Critical Infrastructures	2022
P39	[3]	Toward successful DevSecOps in software development organizations: A decision-making framework	2022
P40	[4]	Expanding devsecops practices and clarifying the concepts within kubernetes ecosystem	2022
P41	[22]	Implementing devsecops pipeline for an enterprise organization	2022
P42	[93]	DevSecOps In Embedded Systems:An Empirical Study Of Past Literature	2022
P43	[7]	Continuous engineering for Industry 4.0 architectures and systems	2022
P44	[39]	Challenges and Opportunities of Devops in Cyber-Physical Production Systems Engineering	2023
P45	[6]	Capabilities and practices in devops: a multivocal literature review.	2023
P46	[35]	Critical success factors for DevOps adoption in information systems development	2023
P47	[16]	Security in DevSecOps: Applying Tools and Machine Learning to Verification and Monitoring Steps	2023
P48	[78]	Seamless Integration of DevOps Tools for Provisioning Automation of the IoT Application on Multi-Infrastructures	2023
P49	[97]	Advanced Persistent Threats and Their Defense Methods in Industrial Internet of Things: A Survey	2023
P50	[1]	Making Sense of Failure Logs in an Industrial DevOps Environment	2023
P51	[96]	Revisit security in the era of DevOps: An evidence-based inquiry into DevSecOps industry	2023
P52	[28]	Design and Implementation of an IIoT Driven Information System: A Case Study	2023
P53	[58]	A systematic mapping study on software testing in the DevOps context	2023
P54	[14]	DevOps for Manufacturing Systems: Speeding Up Software Development	2023
P55	[88]	Automated Security Findings Management: A Case Study in Industrial DevOps	2024
P56	[54]	Industrial Challenges in Secure Continuous Development	2024
P57	[13]	IoT-Driven Innovations: A Case Study Experiment and Implications for Industry 5.0	2024

A. RQ1:RESEARCH TRENDS OF DEVOPS OR DEVSECOPS IN INDUSTRY 5.0

In recent years, research studies on DevOps or DevSecOps in Industry 5.0 have shown a growing trend in publications. The concept of Industry 5.0 has garnered significant attention from academics, Industry, and practitioners, resulting in an increasing number of publications on this topic.

This research topic attempts to determine the level of scientific interest through publications and the kind of scientific journal in which the use of DevOps or DevSecOps in Industry 5.0 has been published. To see the academic

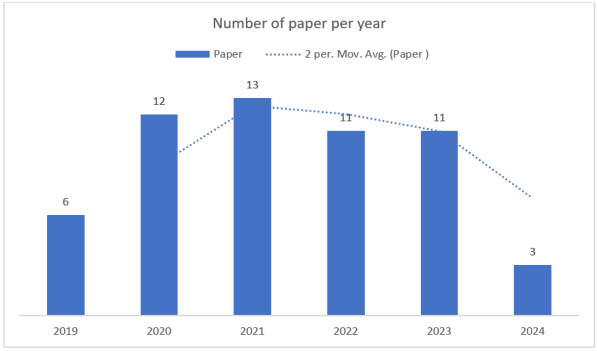

FIGURE 3. Number of primary studies selected published per year.

publications based on the use of DevOps or DevSecOps in the Internet of Things in Industry 5.0, particularly in Industrial Internet of Things, the appropriate journals, conferences, and workshops where they are published, and the various ways they have contributed throughout time.

1) FREQUENCY OF PUBLICATIONS

The papers chosen for this study were examined to identify publication trends and thematic development. Figure 3 displays the annual number of articles when researchers began investigating the application of DevOps or DevSecOps in Industry 5.0. The findings indicate that from 2019 through 2023, there will be an average of 12 publications per year, ranging from 6 articles in 2019 to 13 in 2021 indicating a growing interest among researchers and practitioners in the integration of DevOps or DevSecOps in Industry 5.0.

2) PUBLICATIONS VENUES

To find a place where research findings or articles are shared and spread new knowledge and discoveries in our work. We give some journals, conferences, or an online platform where publications are done in Table 2 and Figure 4. We have discovered that most research papers are disseminated through conference publications, followed by journals. 47% of the studies, equivalent to 27 research articles, were disseminated through conference proceedings, while 40% represents 23 research articles published in journals, and 7 research articles equivalent to 12% of the workshop papers were found published.

Figure 4 illustrates the distribution of papers per venue and year. We can see from the figure that Journals and Conferences are the best places for articles to be published, followed by workshops.

Nevertheless, the limited quantity of publications found in these highly regarded journals fails to substantiate definitive conclusions regarding their significance.

As Industry 5.0 advances, prospective research endeavors might be able to derive such findings from more extensive collections of pertinent literature.

TABLE 3. Number of publications venues selected on DevOps or DevSecOps for Industry 5.0.

List of selected venues		
Publications	**# Studies**	**Studies**
Conference	27	P02, P03, P04, P07, P08, P09 P12, P15, P16, P20, P23, P25, P33, P35, P37, P38, P40, P41, P42, P44, P47, P48, P54,P55, P56, P57
Journal	23	P01, P05, P10, P13, P14, P21, P27, P28, P29, P30, P31, P32, P34, P39, P43, P45, P46, P49, P50, P51, P52, P53
Workshop	7	P06, P11, P17, P22, P24, P26, P36

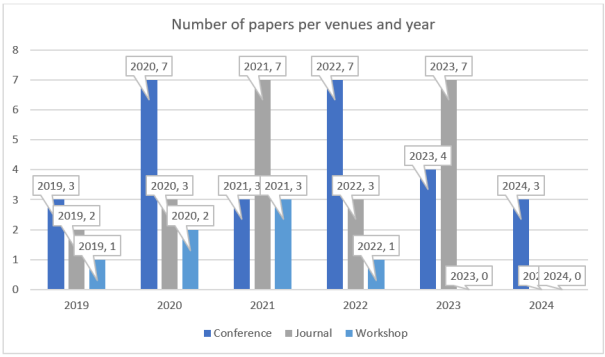

FIGURE 4. Number of primary studies selected published per venues and year.

The Top 10 conferences that focus on DevOps and DevSecOps in Industry 5.0 are highlighted in Table 4 and are considered to be the most popular.

These conferences also account for a significant portion of all conference publications related to this field. It is worth noting that conferences with an equal number of publications are arranged in alphabetical order based on their full names.

The large number of conference papers means that there are more and more important publications related to the adoption of DevOps and DevSecOps for software development in Industry 5.0.

Table 5 illustrates the top 10 journals that have gained significant popularity, with a notable contribution in the published journal papers. In cases where multiple journals have produced an equal number of publications, they are appropriately portrayed based on their respective names.

3) COUNTRY AND INSTITUTION CONTRIBUTING TO THE FIELD

We have discovered that 25 publications, accounting for 44% of the total include German researchers. Following closely authors from the USA, contributing 35 publications, Austria with 29 publications, and France with 28 publications, as illustrated in Figure 5. In total, 17 countries have contributed to research on DevOps and DevSecOps for Industry 5.0 with a combined output of 57 contributions. It is important to note that papers with authors from multiple

TABLE 4. The top 10 conferences of publications on DevOps or DevSecOps for Industry 5.0.

List of Top 10 selected Conferences	
Conference Full Name	**# of Studies**
International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP)	3
IEEE International Conference on Software Architecture Companion (ICSA-C)	3
International Conference on the Internet of Things,	3
International Workshop on Software Engineering Research and Practices for the IoT (SERP4IoT)	2
International Conference on Sensing and Instrumentation in IoT Era (ISSI)	3
IEEE International Conference on Smart Internet of Things (SmartIoT)	3
International Conference on Software Engineering and Computer Systems	3
Euromicro Conference on Software Engineering and Advanced Applications (SEAA)	3
International Conference on Software Engineering: Companion Proceedings (ICSE-Companion)	2
International Conference on Software Architecture Companion (ICSA-C)	1

TABLE 5. The top 10 journals of publications on DevOps or DevSecOps for Industry 5.0.

List of Top 10 selected journals	
Journal Full Name	**# of Studies**
Sensors	3
Information Technology	2
IEEE Internet Things	2
IEEE International Congress on Internet of Things (ICIOT)	2
IEEE Access	2
Information and Software Technology,	2
Information	2
Systems and Software Security and Protection	2
Software Impacts	1
Transactions On Software Engineering	1

countries are counted as multiple-country contributions. Among these, the Top 10 countries, which are the most active in publishing, have produced 32 publications, making up 56% of the total. Furthermore, out of these 32 contributions, 35 (61%) are from European countries. This indicates that the practice of DevOps and DevSecOps in Industry 5.0 predominantly remains a European research endeavor. Despite launching associated initiatives in various nations throughout the globe. It is important to note that we have also discerned the organizations displaying the highest levels of involvement in the study of DevOps and DevSecOps for Industry 4.0. Overall, the field benefits from the contributions of 28 institutions. Given that Germany is the birthplace of the term Industry 5.0 and that 49% of the publications in this field have German co-authors, it is to be expected that 6 out of the 10 most active institutions in this field are from Germany.

4) TYPE OF RESEARCH HAS BEEN DONE ON DevOps OR DevSecOps

In this section, we focus specifically on the application of DevOps and DevSecOps in Industry 5.0, In Figure 6, it is illustrated that DevOps and DevSecOps are being implemented in various types of authorship. The predominant

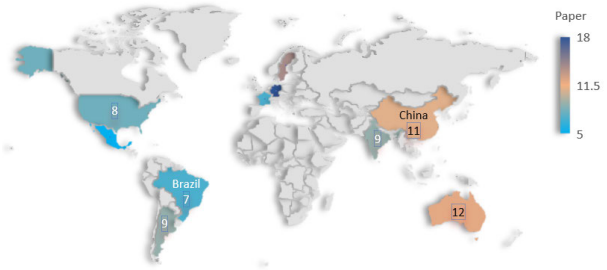

FIGURE 5. The countries that actively publish the most with authors contributing to DevOps or DevSecOps in Industry 5.0 are primarily located in Europe and account for 61% of the publications.

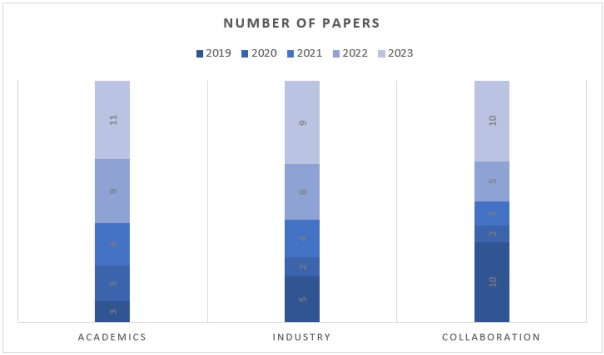

FIGURE 6. Number of papers based on authorship type in this study.

usage of DevOps and DevSecOps can be seen in academic research, with 33 articles or 57% of the total, followed by 30 articles on collaboration between the academic and industry sectors. The industry research with 28 articles is equivalent to 49%. This trend is marked by the fact that there is a strong interest in the Internet of Things. The pharmaceutical industry is exploring the use of DevOps methodology, as well as implementing the DevOps and DevSecOps approach in software development. The industry sector also includes the robotics system, which forms a part of the embedded systems and vehicle sector. DevOps is a methodology that is being researched and applied in Industry 5.0, particularly in the manufacturing sector, L'Esteve [46] focuses on the monitoring and maintenance of manufacturing machines. Additionally, DevOps is also being studied and applied in other sectors such as oil and gas (O&G) and Digital Twin, Elijah et al. [24] and Atif [8] being the respective researchers.

5) APPROACH, CONCEPT, AND METHOD APPLIED ON DevOps OR DevSecOps RESEARCH

Applied DevOps research in the context of Industry 5.0 has several specific approaches, concepts, and methods of interest. There is a focus on applying DevOps and DevSecOps practices and principles, which involves using continuous integration/continuous delivery (CI/CD) pipelines, and distributed version control to coordinate the building, testing,

TABLE 6. Approach, concept, and method interest for applied DevOps research in Industry 5.0.

DevOps practices	#Papers	Ref.
Continuous Integration	22	[P11, P13, P14, P17, P22, P25, P23, P24, P25, P28, P33, P35, P37, P38, P42, P47, P49, P51, P53, P55, P56, P57]
Continuous delivery	14	[P08, P17, P24, P25, P27, P28, P29, P32, P34, P37, P38, P43, P47, P49]
Continuous Deployment	12	[P17, P18, P19, P23, P25, P26, P28, P29, P31, P32, P34, P45]
Microservices architecture	5	[P11, P34, P33, P16, P24]
Automated testing	5	[P08, P24, P18, P16, P23]
Automated deployment	4	[P34, P17, P16, P23]
Continuous monitoring and measurement	4	[P34, P33, P34, P23]
Infrastructure As Code	5	[P22, P05, P44,P34]

and deployment of software services in Industry 5.0 as presented by Pando and Dávila [58].

It can be inferred from Table 5 that continuous integration is widely used in Industry 5.0. According to the Table 6, 22 papers (42%) have employed continuous integration. However, 14 papers (24%) have also used continuous delivery to address activities, and 12 papers (21%) in continuous deployment.

Infrastructure as code (IaC) [P11] is also a significant area of research, with topics such as frameworks/tools for IaC, being explored as described by Rahman et al. [65] with 5 papers. The following table presents the specific areas of interest for applied DevOps research in Industry 5.0.

The integration of machine learning (ML) techniques into industrial production processes, also known as MLOps has research interest. Research suggests that MLOps in Industry 5.0 encounter similar challenges to those in pure software systems.

A bibliometric analysis was conducted in Figure 7 to investigate the progression of scholarly data through the primary keywords. The examination of bibliometric results utilizing the scientific tool VOSviewer is focused on recognizing the principal research terms such as DevOps and DevSecOps and Industry 5.0.

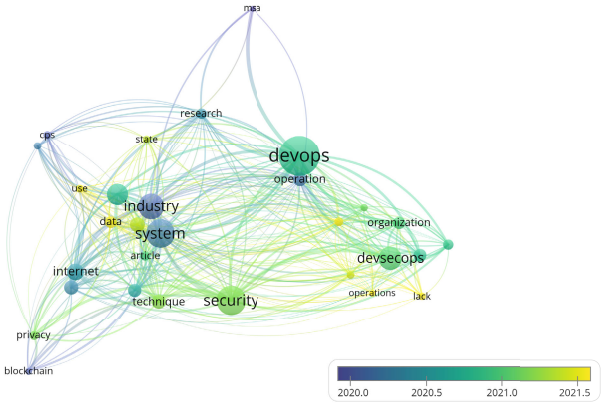

FIGURE 7. Network of all keywords applied DevOps in Industry 5.0. Source: own elaboration.

B. RQ2:BENEFITS OF IMPLEMENTING DevOps IN INDUSTRY 5.0

DevOps in Industry 5.0 provides multiple advantages in the realm of industrial systems. We have organized our research findings into three primary benefits themes: Organizational, Technical and regulatory. Table 7 displays the benefits of using DevOps and DevSecOps in Industry 4.0, as identified through the selected studies. The first column contains the categories, the second column the IDs, and the third column contains the benefits and studies that mention each benefit.

- *Organizational*: This topic addresses the benefits related to knowledge and skills, multidisciplinary collaboration, and organizational culture that can be beneficial to DevOps or DevSecOps in Industry 5.0.
- *Technical*: This topic discusses technical matters related to the benefits to DevOps or DevSecOps practices in industry 5.0, comprising continuous integration and continuous deployment (CI/CD) and integration of security practices.
- *Regulatory*: This topic discusses the benefits of implementing DevOps in Industry 5.0's regulatory landscape.

1) ORGANIZATIONAL BENEFITS

We observe several studies that have explored the benefits of DevOps and DevSecOps domains in the Industrial environments [P03, P08, P17, P05, P28, P44]. As presented in Table 7, this section focused on the organizational benefits of adopting DevOps and DevSecops in Industry 5.0.

1) *BE01:Organizational improvements*
Implementing DevOps in an organization improves the efficiency and productivity of software development and deployment [P17]. By leveraging the diverse skills and perspectives of team members, organizations can achieve innovative and continuous improvement in their software development and deployment processes. Implementing DevOps involves continuous backlog prioritization and quality evaluation, which can result in earlier product delivery and improved organizational flexibility [P17]. An organization increases flexibility in planning activities. Integrating stakeholders, systems, and data through incremental steps and making quick adjustments allows rapid adaptation to changing requirements and market demands, providing greater flexibility in industrial production environments.
2) *BE02: Collaboration between Teams*
Several studies [P33, P22, P28] revealed that implementing DevOps practices in industrial environments improves communication and coordination between different teams. It also facilitates the sharing of knowledge, expertise, and ideas, which ultimately leads to better problem-solving and decision-making

processes [P28]. DevSecOps encourages collaboration between development, security, and operations teams [P17]. In the context of industrial IoT, this means that these teams work together to design, develop, and deploy secure industrial IoT solutions from the outset. A culture of teamwork and shared responsibility is fostered, which promotes a sense of ownership and accountability among team members and relies on collaboration among different roles and responsibilities [P17].

Many papers [P28, P44] emphasize the benefits and challenges of implementing DevOps in CPS environments. It has been reported that the integration of continuous software engineering practices like DevOps offers several advantages, such as enhanced communication and collaboration between developers and customers, increased productivity, better product quality, and greater infrastructural independence. This was discussed by Kan et al. [38].

The authors [P28] agree that It enables cross-functional teams to work together more effectively, breaking down silos, and thus facilitating the exchange of information and feedback throughout the SDLC.

2) TECHNICAL BENEFITS

The technical benefits of adopting DevSecOps in Industry 5.0 are described by the benefits as referenced in Table 7.

3) *BE03: Supporting multiple architectural*
Numerous studies mentioned that DevOps and DevSecOps support multiple architectural in industrial in regulated environments, It emphasizes the use of containerization and microservices, which are known for their scalability and flexibility. It ensures the security of containerized applications and microservices by incorporating security checks and policies into the deployment pipeline [P17].
According to Igor et al. [P22], utilizing cloud computing in IoT projects that utilize DevOps during their construction can result in high availability of services. Furthermore, it can provide greater agility in meeting requirements such as scalability, elasticity, disaster recovery, and security.

4) *BE04: Supporting secure deployment*
DevSecOps plays a vital role by automating the build, test, and deployment processes, which ultimately leads to a streamlined development lifecycle and a reduction in time spent on these stages [P28, P22, P17, P33]. A study [28] revealed that adopting Secure DevOps would significantly impact the entire lifecycle of CPS development processes. It would extend the security coverage to all phases, including system development, device deployment and provisioning, standard operations, maintenance, and system dismissal. It facilitates automated deployment tools by incorporating automated static and dynamic security testing to identify vulnerabilities and ensure the security of the system. Adopting Secure DevOps aids in achieving faster, more cost-effective, and more efficient development and maintenance of secure CPS. Additionally, they could provide more frequent and safe updates to software under a wide range of circumstances with increased reliability of the process [P28].

5) *BE05: Facilitate integration of the security standard*
Researchers [P28, P17, P33, P31] agree that implementing DeveSecOps in industrial environments facilitates the integration of security standards, industry-standard protocols, and technologies, and promotes interoperability. Standards such as OPC UA (Unified Architecture) provide a common framework for communication and data exchange between various devices and systems. It facilitates security policy design and performance measures, compliance, and policy [P08, P31, P38]. Incorporating DevSecOps in Industrial IoT can help integrate security at every phase of the IoT lifecycle, enabling proactive security measures, threat prediction, detection, and alerting mechanisms [P24, P38, P17].
The successful implementation of DevSecOps in an industrial setting demands strict adherence to well-defined security policies that specify the permissible communication between devices connected to the network.
It supports secure coding standards that serve as an effective method to address the security challenges faced by industrial systems and that support critical infrastructures [P08, P17, P24, P16, P31]. These systems must adhere to strict security regulations and standards, making the use of secure coding standards essential.

3) REGULATORY BENEFITS

This section describes the regulatory benefits of adopting DevSecOps for Industrial environments.

6) *BE06:Protection of intellectual properties*
Numerous studies [P17, P24, P28, P44] revealed that implementing a secure DevOps framework that complies with security policies can help to safeguard intellectual properties in Industrial environments. This framework ensures the protection of intellectual property and proprietary tools, methods, and techniques, which are often the reasons for operating in a highly regulated environment.

7) *BE07:Traceability across all levels of code branches*
Some Studies [P28, P17] traceability across all levels of code branches refers to the process of ensuring that the Industrial environments comply with regulatory requirements. This can be achieved through implementing end-to-end traceability capabilities and automating the management of artifacts throughout the project life cycle. By doing so, DevOps personnel

can ensure that all code branches are traceable and that all relevant information is documented to maintain transparency throughout the development process.

8) *BE08:Facilitate item identification and audit trails*
Researchers [P17, P28, P08] revealed that the implementation of DevSecOps in Industry 5.0 can aid in the identification of items and the creation of audit trails. DevSecOps improves the security of industrial systems by regulating access to resources through authorization delegation procedures, enabling the auditing of authorizations, detecting misconduct and possible attacks, and ensuring the attribution of misconduct.

9) *BE09: Adapt to new regulations.*
Implementing DevSecOps in Industrial systems ensures compliance with industry standards and regulations [P17, P08]. It provides a framework for managing security and privacy requirements. In regulated environments, implementing DevSecOps allows entities mandated by security policies to conduct their Software Development Lifecycle (SDLC) activities while conforming to all imposed policies. DevOps can improve software quality and adapt to changing contexts [P17]

C. RQ3:CHALLENGES ADOPTING DevOps AND DevSecops IN INDUSTRY 5.0

DevOps and DevSecOps have encountered multiple challenges in the realm of industrial systems. We have organized our research findings into three primary challenge themes: Organizational, Technical, and regulatory. Table 8 displays the challenges of using DevOps and DevSecOps in Industry 5.0, as identified through the selected studies. The first column contains the categories, the second column the IDs, and the third column contains the challenges and studies that mention each challenge.

1) ORGANIZATIONAL CHALLENGES

The challenges detailed in Table 8, CH01 to CH05, describe the organizational obstacles to implementing DevOps and DevSecOps in the industrial environment.

1) *Ch01:Lack of management:*
Numerous studies [P28, P17, P44, P34, P56] found multiple challenges related to DevOps and DevSecops in Industrial environments. Indeed, implementing DevSecOps is challenging due to poor communication, weak collaboration, and lack of management support [P44]. Study [P33] mentioned proper management is necessary when new processes, activities, and automation require collaboration among individuals who are not used to working together.

2) *Ch02:Inter-team collaboration:*
In a recent study [P34], authors revealed that Effective communication and collaboration among teams play a vital role in achieving success in DevSecOps.One of the main issues reported was conflicts between development and security teams regarding collaboration. It can be challenging in CPS engineering due to the diverse backgrounds and expertise of the engineers [P44]. Another obstacle encountered in the engineering and operation of CPS is the absence of connectivity in rural or remote areas [P39]. When individuals switch from one role to another, they often face various challenges such as resistance to change and uncertainty [P33]. It is hindered in highly regulated development due to siloed organizations, centralized repositories, network security restrictions, and external integration complications [P17]. The silo-based work culture in the software community hinders frequent and effective communication and collaboration between stakeholders, creating a barrier to secure DevOps [P34].
In embedded systems development, teams often work in specialized module teams or silos, with limited communication and collaboration between teams [P42].

3) *Ch03:Organizational culture*
To successfully adopt DevSecOps, several cultural and behavioral changes must be made. The authors [P33, P44] mentioned that challenges in organizational culture, such as resistance to change [P33] and cultural barriers [P34] within the organization, can impede the successful implementation of DevOps, as it requires a change in mindset and collaboration between different teams. Some organizations face challenges related to their culture when it comes to prioritizing security. Reluctance to give importance to security is one such challenge that has been reported [P34].
DevSecOps is closely aligned with Agile development principles, which emphasize iterative development, continuous feedback, and collaboration with stakeholders. However, embedded systems development has traditionally followed a more waterfall or sequential approach [P42].

4) *Ch04:Communicate security standards with the DevOps team*
The organization establishes security standards to be followed when using technologies. These standards are the requirements that must be met to comply with the security policy while performing operations. It is necessary to communicate these standards to the DevOps team when working on security[P39]. According to researchers [P39, P44, P08, P34], cybersecurity specialists need to communicate security standards to the DevOps team and share incident data and other relevant information with team members and relevant institutions. The application's security standards must be considered in the development process. Ignorance of these standards can hinder development tasks [P39].

5) *Ch05:Education and Training*
The rapid evolution of hacking techniques and the constant threat of cyber attacks pose significant challenges

TABLE 7. List of benefits when adopting DevOps and DevSecops in IIoT.

List of Benefits		
Benefits	**No**	**Categories and Papers which contributed to the categories**
Organizational Benefits	BEO1	Organizational improvements [P17, P56]
	BE02	Collaboration between teams [P17, P28]
Technical benefits	BE03	Supporting multiple architectural [P17, 28]
	BE04	Supporting secure deployment [P17]
	BE05	Facilitate integration of security standard [P17, P28]
Regulated benefits	BE06	Protection of intellectual properties [P16, P17]
	BE07	Traceability across all levels of code branches [P34, P12]
	BE08	Facilitate item identification and audit trails [P56]
	BE09	Adapt to new regulations [P17,P16, P56]

in protecting confidential information and identifying cyber threats in industrial IoT environments. Several authors [P33, P34, P56, P17, P08, P44] have highlighted the challenge which refers to the lack of security education and training [P33, P34], as well as the shortage of security experts. These factors hinder the effective implementation of cybersecurity measures. Addressing these challenges requires a comprehensive understanding of the specific security needs of industrial IoT systems. Furthermore, specialized training programs need to be developed to educate practitioners on implementing secure DevSecOps practices in regulated environments [P34]. One of the challenges of incorporating DevSecOps into CPPS is the need for specialized skills and knowledge, particularly in security engineering and risk management [P44].

2) TECHNICAL CHALLENGES

This section lists the technical challenges of adopting DevSecOps in the industrial environment.

6) *CH06: Automated testing tools for security in DevOps*
Testing is a crucial aspect of software development as it helps to identify and eliminate any defects or bugs before the product is delivered to the client, ensuring that the final software product is of high quality. The DevOps process of continuous development involves the use of automated testing tools and knowledge of security protocols to validate software builds before they are added to a repository [P39]. M.A. Akbar et al. [P39] found that many security issues in DevOps software development arise due to a lack of automated testing tools or a lack of awareness regarding static testing for security. Heterogeneous hardware and software interfaces and communication systems in CPS pose challenges to automating testing, integration, and deployment [P44]
7) *CH07: Define security parameters and management.*
There is no consensus on how to integrate security measures into the DevOps pipeline in a way that establishes robust mechanisms for incorporating security by design within existing DevOps practices. The challenges of secure software deployment are exacerbated by basic security measures and the potential for man-in-the-middle attacks.
8) *CH08: Difficult to adopt DevSecOps in complex cloud environments.*
DevSecOps principles and practices are challenging to adopt in complex cloud environments of various types [P34]. Producing secure software in a cloud environment for a system-of-systems (SoS) target is challenging due to its complexity [P34]. There is a lack of interoperability between different cloud solutions, which increases the complexity of maintaining and evolving complex applications deployed across multiple cloud infrastructures and platforms. Architecture such as microservices and automated distributed deployments, which are heavily utilized in multi-cloud environments, have made security assurance challenging. Studies also report that data security is another critical issue in this domain [P34].
9) *CH09: Resistance to integration of security.*
DevOps requires security methods that differ from traditional approaches. However, creating a security culture within DevOps teams requires overcoming resistance to behavioral changes [P39]. Current DevOps and security tools are often too complex for developers without security expertise [P34]. Developers often prioritize delivering products on time over integrating security protocols [P39].
10) *CH10: Challenges related to security practices in rapid deployment environments.*
Due to the continuous and rapid software releases, measuring security in the DevOps paradigm becomes even more challenging [P34]. DevOps can be challenging for systems that require strict security measures, slowing down the process. One challenge with security measurement in rapid deployment environments is the use of slow data gathering methods. Fast feedback loops are essential for CD systems [P34]. Quick feedback loops between DevSecOps teams and project stakeholders are important. However, the implementation of these processes faces various challenges from using traditional methods to cultural issues.
11) *CH11: Challenges related to tool selection*
In the DevSecOps paradigm, the use of tools is highly encouraged. Several tools have been developed to cater to all stages in the DevSecOps process [P34]. Each team member has different preferences for tools,

leading to varied choices within and across teams. Automated software security testing tools are necessary to ensure security in rapid deployment environments. The tool-centric nature of DevSecOps and the availability of a substantial number of tools exacerbate the challenge related to the security automation goal of this domain, which is the lack of standards for tool selection [P34].

12) *CH12: Lack of secure coding standards*
More research [P34, P33, P56] is needed on the systematic application of security standards in DevOps. Due to the increased exposure of sensitive and safety-critical operations to the broader cyber environment, there has been a surge in malicious attacks on industrial processes. Industrial control systems that support critical infrastructures must comply with rigorous security regulations and standards, making it challenging to implement DevOps practices [P08].

3) REGULATORY CHALLENGES

13) *CH13: Adopting DevOps and DevSecOps in highly regulated environments*
Implementing DevOps practices in highly regulated environments can be challenging due to strict policies and regulations that need to be followed [P34]. HRE have policies in place to ensure the overall security of their operations and protect intellectual property [P17]. These policies may include requirements for secure software development practices and data protection. HRE may also need to comply with industry-specific regulations, such as HIPAA for healthcare, PCI DSS for the payment card industry, or NIST standards for government agencies. Implementing traditional DevSecOps concepts can be challenging for embedded systems due to increased regulations and standards. Embedded systems, especially those used in regulated industries such as medical devices or automotive, are subject to strict compliance and regulatory requirements [P42].

14) *CH14: Identify software defects*
Configuration management a process that includes updating software, version control, incident handling, and defect tracking poses challenges. To identify vulnerabilities in an application, organizations must conduct penetration testing [P39]. Once vulnerabilities are detected, they should be reported to the development team for defect management [P39]. Secure deployment parameters and configurations must be implemented to ensure control over security operations.

15) *CH15:Continuous security assessment*
It is recommended to perform continuous security assessment in DevSecOps, but related processes are not commonly adopted, including continuous vulnerability assessment [P34]. Continuous security assessment poses challenges, it is necessary to have clear instructions on which sections of the pipeline should be included in the security measures. However, there is a lack of consensus and standardized methodology on how to include security measures in a DevOps pipeline [P34].

D. RQ3:PROPOSED ADOPTION OF DevOps AND DEVSECOPS PRACTICES IN INDUSTRY 5.0

This research investigates the types of contributions in the literature regarding adopting DevOps and DevSecOps in Industry 4.0. Table 9 outlines the contribution types found in the primary studies. The most prevalent type was frameworks, methods, and techniques, making up 50% (28/57) of the literature. These studies offered practical solutions for implementing and managing DevOps or DevSecOps in industrial systems. The second most frequent type was lessons learned, accounting for 26% (15/57) of the contributions. Tools constituted 14% (8/57) of the contributions, covering studies that provided a specific technology, application, or program to support DevOps or DevSecOps in industrial systems.

The advice/implications category accounted for 10% (6/57) of the considered contributions, containing discursive and generic recommendations based on personal opinion. On the other hand, guidelines intended to assist practitioners in industry and models representing an abstraction of reality through a conceptualization process each made up (12/57 and 13/57, respectively) of the total contributions.

1) RESEARCH TYPE ON THE ADOPTION OF DEVOPS AND DevSecOps IN INDUSTRY 5.0

This section focuses on the research types and methods used in the literature on the adoption of DevOps and DevSecOps in Industry 5.0. Table 10 provides the research types found in the literature. *Evaluation research* was the most common type, making up 43% (25/57) of the primary studies. These studies typically presented the implementation and evaluation of a solution in practice, using methods such as case studies, surveys, mixed methods, or other empirical approaches. *Solution proposals* were the second most frequent research type, accounting for 22% (13/57) of the studies. These propose new solutions or significant enhancements of existing ones, with their applicability investigated through demonstration, example, or argumentation. *Experience papers* constituted 15% (9/57) of the primary studies, sharing industry-based experiences and practical applications. *Validation research* was conducted in only 10% (6/57) of the primary studies, involving investigations of specific techniques or solutions using methodologically sound research designs, such as experimentation (controlled or quasi-experiments), formal analysis, or simulation.

Opinion papers formed 14% (5/57) of the total, comprising studies that expressed the personal views of experts on specific techniques and their application. *Philosophical papers*, which offer novel perspectives on existing topics and aid DevOps and DevSecOps software engineers in understanding problem areas through conceptual frameworks

TABLE 8. List of challenges adopting DevOps and DevSecOps in Industry.

List of Challenges		
Challenges	**No**	**Categories and Papers which contributed to the categories**
Organizational challenges	Ch1	Lack of management [P28, P34]
	Ch2	Inter-team collaboration issues [P34, P44]
	Ch3	Challenges in organizational culture [P34, P28,P56]
	Ch4	Communicate security standards to the DevOps team [P34, P56]
	Ch5	Lack of security education and training [P56]
Technical challenges	Ch6	Lack of automated testing tools for security in DevOps [P34, P28, P55]
	Ch7	Define secure deployment parameters and management [P34, P28]
	Ch8	Difficult to adopt DevSecOps in complex cloud environments [P34, P44]
	Ch9	Resistance to integrating security [P17, P34]
	Ch10	Challenges related to security measurement practices in rapid deployment environments [P34]
	Ch11	Challenges related to tool selection [P56]
	Ch12	Lack of secure coding standards [P56, P17]
Regulated challenges	Ch13	Difficult to adopt DevOps and DevSecOps in highly regulated environments [P17, P16]
	Ch14	Identify software defects [P34, P28]
	Ch15	Continuous security assessment [P34,P56]

TABLE 9. Contribution type (proposed by Shaw [77] and Paternoster et al. [60].

Title	Description	studies
Framework/ Method/ Technique	The study proposes a framework, method, or technique for facilitating DevOps or DevSecOps construction and management in Industry 5.0.	P02, P03, P04, P06, P08, P13, P23, P24, P25, P27, P28, P31, P38, P39, P54, P49, P35, P36, P45, P34, P26, P55.
Guideline	This is a list of advice and recommendations based on synthesizing the research results.	P04, P17, P04, P06, P25, P13, P26, P11, P45, P53, P24, P19, P46
Lesson Learned	The set of outcomes directly based on the research findings obtained through data analysis.	P09, P35, P35, P45, P53, P51, P56, P35, P26, P26, P27, P28, P49, P41, P43
Model	The process of conceptualizing an observed reality into related concepts or representations.	P52, P32, P32, P42, P52, P56, P13
Tool	A software program or application designed to support various aspects of software engineering.	P41, P52, P35, P57, P25, P39, P47, P38
Advice/ Implication	Here is a recommendation based on personal opinion, which is general and may include a discussion of different viewpoints.	P54, P53, P42, P12, P24, P42

or taxonomies, made up 10% (6/57) of the total. This category encompassed opinion papers, experience papers, and solution proposals, with the majority being philosophical papers. The most commonly employed research method was the case study, featured in approximately 40% (20/57) of the primary studies, particularly in evaluation research. Controlled or quasi-experimentation, the second most frequently used research method, was utilized in 5% (3/57) of the primary studies, primarily within validation research.

2) DEVOPS AND DevSecOps IN INDUSTRY 5.0

The integration of DevOps and DevSecOps practices in the Internet of Things (IIoT) is a topic of great interest to researchers and practitioners. It involves incorporating DevOps principles and methodologies into IoT systems to improve their design, implementation, and operationalization. 15/57(27%) of our primary studies [P03, P06, P10, P15, P19, P22, P31, P33, P48, P49, P52, P57] presented in Table 1 focused on DevOps or DevSecOps in IoT.

3) DEVOPS IN OTHERS INDUSTRIAL PRODUCTION

In recent years, the rapid advancement of DevSecOps technologies has transformed software development and cybersecurity. Several studies [P24, P27, P32, P42, P50, P51, P54, P57] that explore DevOps and DevSecOps in the manufacturing industry have experienced a positive change in product release speed and quality due to the adoption of DevOps methodologies. Morales et al. [P11] propose a guide designed to help adopt DevSecOps infrastructure for supporting systems development in Highly Reglemented Environments. Study [P17] describes that DevOps can adapt to new regulations and increase the competitive capabilities of companies. According to Martin et al. [P17] implementing DevOps in medical device development could result in several improvements compared to traditional development. DevOps can extend and accelerate feedback loops, reduce costs in terms of time and human resources, and decrease the number of defects.

- **Continuous Integration(CI):** Continuous integration (CI) is widely adopted in the software development industry. It has become a standard practice for teams to continuously integrate their code changes into a shared repository and run automated tests to ensure the stability and quality of the software. Several studies have been conducted to analyze the adoption and impact of CI in industrial settings [P36, P03, P05, P08, P09, P10, P14, P16, P46, P42, P45, P48, P50, P56]. Agile is one of the most adopted methods used to implement CI. 54% adopted agile as a method.
  Agile methods [P54] can help with better iteration management and a sustainable pace in system development through regular iterations. According to Morales et al. [P11], tools like ticketing systems,

TABLE 10. Research type (proposed by Wieringa et al. [91]).

Title	Description	Papers
Solution Proposal	A proposed solution for a given problem is presented, which may be either an innovative approach or a substantial enhancement of an existing solution. The potential advantages, limitations, and applicability of this proposed solution are described through a brief example, illustrative demonstrations, or through persuasive argumentation.	P04, P43, P03, P45, P23, P45, P36, P25, P20, P27, P10, P21, P24, P56,
Validation Research	A novel solution or technique is put forth, yet to be implemented in practice. The proposed method is meticulously explored through a rigorous research approach, such as experimentation, prototyping, formal analysis, simulation, or similar methodologies.	P11, P16, P19, P30 P01, P24, P30, P34, P41, P42, P47
Evaluation Research	A novel solution or technique is seamlessly integrated into practical applications (solution implementation), followed by a comprehensive assessment of its effectiveness (implementation evaluation). The feasibility and implications of the solution or technique are thoroughly examined, highlighting both the benefits and potential drawbacks, within a real-world context.	P01, P24, P16, P39, P42, P56, P47, P38, P39, P34, P16, P18, P35, P54, P26, P27, P47
Philosophical Paper	These studies offer fresh perspectives on established domains by systematically organizing a specific field, proposing innovative theoretical structures, or providing a comprehensive taxonomy.	P42, P16, P47, P24
Opinion Paper	These studies offer subjective insights from the author regarding the effectiveness of specific techniques, often without grounding their opinions in established research or a systematic methodology.	P30, P16, P34. P41, P47
Experience Report	These studies share practical experiences and describe how specific techniques have been applied in real-world settings. These accounts often reflect the personal perspectives of the authors, who provide firsthand accounts of their own experiences without explicitly mentioning research methods.	P42, P16, P47, P24. P02, P05, P15, P25, P35

document repositories, schedules, progress monitors, and metrics help all stakeholders track overall progress in software projects. Adopting Agile software development practices is highly recommended for IoT projects because it reduces costs, increases productivity, and shortens time-to-market, as presented by Wouter et al. [98]. In [P18], it suggests that implementing DevOps practices within the Scrum framework can effectively and promptly address the requirements of Industry 5.0. Automation is a method for automating the process of integrating code changes. 46% of studies found that using automation in their process facilitated the more frequent merging of code changes for developers.

- **Continuous Delivery (CD):** Continuous integration (CD) is another topic of DevOps that is widely adopted in the software development industry. Continuous delivery was used by more than 56% of the studies [P04, P05, P11, P22, P24, P25, P26, P29, P31, P34, P35, P38, P41, P42, P43, P57] to automatically release validated code to a repository after performing builds, unit, and integration testing in CI. Continuous Delivery (CD) practices practices have been used in the development of Cyber-Physical Systems (CPS). However, CPS development poses some unique challenges. For instance, it involves combining continuous and periodic builds, which can be difficult to manage. 45% mentioned that been used continuous integration for test automation and code release automation. Some studies are related to the use of Continuous Delivery for the process of automatically testing and uploading an application developer's changes to a repository, such as GitHub or a container registry. This enables the operations team to deploy the changes to a live production environment.

According to a study [P28], Implementing DevOps and DevSecOps can reduce the cost [P17] and time of development, operation, and maintenance. This is because bugs and architectural flaws are minimized through an integrated risk management and security view throughout the entire CPS lifecycle.

- **Continuous Deployment (CD):**
Continuous Deployment has been proposed to implement system deployment in DevOps (e.g., rapid deployment, and deployment in production, deployment multi-cloud, and testing environments). Research [P02] findings propose the ongoing implementation of Internet of Things (IoT) platforms through a versatile Docker Compose tool that functions effectively across different settings such as staging, development, deployment, and testing. Study [P40] suggests using Kubernetes working a range of container tools such as Dockers to deploy and scale in production. Study [P49] mentioned that after completing all previous phases, the change is finally deployed to Production. We separate the operations and production as post-deployment is a long-term process that is distinct from the production deployment. Automate Build, Test, and Deployment Processes have been implemented in deployment processes in embedded systems development [P42]. This includes automating code compilation, unit testing, integration testing, and deployment processes [P42].
Study [P24] has proposed continuous deployment for the entire software delivery pipeline in robotics, from code commit to production deployment. According to a study [P28] Companies can ensure the same level of security by adopting a Secure DevOps approach, which could boost agile and continuous development. By providing better security and stability, the improved quality of

service can be achieved [P17] at a more competitive cost [P17], which will enhance the competitive advantages of the companies in the CPS market. This, in turn, enables a significant increase in the business volume and the range of services offered to the market. In [P02], it demonstrates the potential value of automation practices within the context of Industry 4.0 and DevOps solutions.

- **Continuous Monitoring (CM):** Our investigation revealed that many studies have addressed monitoring infrastructure in DevOps practices and have been used in different components of Industry 5.0. 45% of the studies used continuous monitoring to detect suspicious activity, such as brute force attacks, password spraying, and SQL injection, to reduce the risk of cyberattacks. and the other hand Study [P30] underscores the need for continuous monitoring and control, and an ability to adapt to evolving standards and regulations. In the realm of the Industrial Internet of Things (IoT) has applied to involves combining continuous integration, testing, deployment, and delivery, along with version control, monitoring, and alerting at the device level as presented by Bijwe et al. [P24].
  Hasan et al. [P42] revealed that continuous monitoring in embedded systems helps ensure the reliability, security, and optimal performance of the system throughout its lifecycle [P24].
- **Continuous Integrating Security (CIS):** Pekka et al. [P28] mentioned that Integrating security into DevOps gives companies a competitive advantage in a market where IoT services are dominant and cybersecurity is a concern. By prioritizing a secure IoT infrastructure, companies can reduce barriers that prevent the acceptance of IoT solutions. As organizations increasingly adopt DevSecOps practices, integrating security into the software development lifecycle becomes paramount. Study [P28] related that many companies are adopting a Secure DevOps approach to Cyber-Physical Systems (CPS) as it offers a great opportunity to increase price competitiveness by automating and optimizing cost structure in a revolutionary way. Moyon et al. [P08] integrated security standards into DevOps pipelines and validated them for IEC 62443-4-1 standard, regulating the Industrial Control System (ICS) domain. According to [P28, P17] The implementation of DevOps and DevSecOps, companies can produce comprehensive, flexible services with integrated security, leading to significant quality improvements in functionality, extensibility, and defect rates.

4) PROPOSED MATURITY MODELS

Maturity Models are tools used to measure the level of knowledge or performance in a particular process or activity. DevOps maturity models have been explored in the industrial context. Raluca et al. [15] propose a concept for DevOps for manufacturing systems, based on current best practices and the specific situation in the industrial company. The concept was implemented and validated by experts, demonstrating the usefulness of DevOps for manufacturing systems.

Industrial DevOps Maturity Model (IDMM): Bijwe and Shankar [10] discussed the challenges of implementing a DevOps culture in IoT applications and suggested a new model called the Industrial DevOps Maturity Model (IDMM) to provide usage guidelines. IDMM provides guidelines and practices for implementing DevOps in IoT applications. By following the recommended practices and guidelines of the IDMM, organizations can achieve faster deployments with improved quality in their IoT projects. Bijwe and Shankar [10]highlight the importance of continuous integration, testing, deployment, and monitoring in the DevOps methodology for IoT devices.

OWASP DevSecOps Maturity Model (DSOMM)[1]: Raluca et al. [15] OWASP DSOMM focuses on integrating security practices into the DevOps process, ensuring that security is considered throughout the software development lifecycle. It provides a maturity model that helps organizations assess and improve their security practices in the context of DevOps. The model covers various dimensions, including culture, automation, measurement, and sharing, to promote a holistic approach to security in DevOps. It emphasizes the importance of collaboration between development, operations, and security teams to address security concerns effectively. OWASP DSOMM aims to enable organizations to achieve a higher level of security maturity by integrating security into their DevOps practices and processes.

Building Security In Maturity Model (BSIMM)[2]: Raluca et al. [15] BSIMM is a model proposed by Synopsys that aims to measure and improve software security maturity. It provides a framework for assessing an organization's software security practices and comparing them to industry best practices. The model consists of four main dimensions: Governance, Intelligence, SSDL Touchpoints, and Deployment. Each dimension includes various subdimensions and activities that focus on different aspects of achieving software security. BSIMM helps organizations define a roadmap to improve their security initiatives and provides a benchmark to compare their practices with other companies.

E. RQ5:DevSecOps TOOLS AND TECHNIQUES TO PROVIDE SECURITY AND SAFETY IN INDUSTRY 5.0?

The answer is to investigate current DevSecOps tools and techniques from the literature and industry to provide security and safety in Industry 5.0. DevOps and DevSecOps in Industry 5.0 are implemented using a variety of tools and technologies.

[1]https://owasp.org/www-project-devsecops-maturity-model/
[2]https://www.synopsys.com/software-integrity/software-security-services/bsimm-maturity-model.html

TABLE 11. Devops tools.

DevOps Practice	DevOps Tools	Papers
CD	Jira, Git, Maven, Gravel, Junit, Se	P01, P03, P17, P21, P14, P16 , P34, P41, P04
CI	Jira, Git, Maven, Gravel, Junit, Se, Docker, Puppet, Chef, Ansible, SalTrac	P01, P04, P06, P09, P08, P34, P43, P26, P48
CD	Docker, Puppet, Chef, Ansible,SalTrac	P02, P06, P4, P14
CM	Stack, Nagios	P23, P08, P34, P19

These include GitLab code management, Jenkins pipeline technology, docker container technology, Kubernetes container orchestration technology, and other prevalent tools that have been used such as Ansible, and Git as described by Ebert & Hochstein [99].

These tools work together to form the DevOps platform, which enables continuous integration, continuous delivery, and continuous deployment as specified by Chen and Suo [17]. Additionally, cloud-native technology is utilized to design and apply an integrated operation and maintenance platform, improving research and development efficiency. The following table presents the list of tools used in Devops to provide security and safety in Industry 5.0.

1) DevSecOps SECURITY TOOLS

This research has delineated thirteen classifications of security tools employed within the realm of DevSecOps. Each of these classifications can be further segmented into subcategories, and the classification of specific security tools may vary depending on the source. The subsequent sections provide a concise overview of the categorized security tools outlined in this study, as shown in Table 9

DevSecOps includes a variety of application security testing (AST) tools that are integrated into different stages of the CI/CD process. These tools include Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), IAST, Infrastructure as Code (IaC), and Software Composition Analysis (SCA). The commonly used security tools are listed below:

1. **Static Application Security Testing (SAST):**. SAST is a code analyzer used during software development to detect coding errors and design flaws that could lead to exploitable vulnerabilities [P08, P24, P51, P54].In the context of robotics development, SAST can be applied during the development phase of the DevSecOps cycle, and plays a crucial role in identifying security vulnerabilities in the source code during the development phase of the DevSecOps cycle in robotics [P24].
2. **Software Composition Analysis (SCA):** Component vulnerabilities are detected continuously from integration to production release through the use of source code and binary analysis, providing security risk information integrated into the CI/CD process [P24]. By incorporating SCA into the DevSecOps cycle, roboticists can proactively identify and address potential security risks associated with the software components used in their projects [P24]. This helps in building more secure and resilient robotics systems.
3. **Interactive Application Security Testing (IAST)**. This tool analyzes application behavior at runtime during manual or automated functional testing. It is a testing methodology that combines elements of both dynamic application security testing (DAST) and static application security testing (SAST) [P08, P24, P51, P54]. It is a form of black-box testing that assesses the security of an application while it is running. In IAST, the application is instrumented with security sensors or agents that monitor its behavior and interactions with the underlying infrastructure. These sensors capture runtime data, such as inputs, outputs, and network traffic, and analyze it to identify potential security vulnerabilities and weaknesses [P08, P51, P54]. IAST is a valuable addition to the DevSecOps approach in robotics development. By incorporating IAST into the testing phase, roboticists can gain deeper insights into the security of their applications and identify vulnerabilities that may not be easily detectable through other testing methods. This helps in building more secure and resilient robotics systems [P24].
4. **Dynamic Application Security Testing (DAST):** Dynamic Application Security Testing (DAST) is a testing methodology used to assess the security of an application by analyzing its behavior in a running state. It is a black-box testing technique that simulates real-world attacks on the application to identify vulnerabilities and weaknesses [P08, P54, P24, P51]. DAST involves testing the application from the outside, without access to its source code. It interacts with the application through its user interface or exposed APIs, sending various inputs and analyzing the responses to identify potential security vulnerabilities [P24, P51]. DAST simulates different types of attacks, such as injection attacks, cross-site scripting (XSS), SQL injection, and more. It sends malicious inputs or payloads to the application to see how it responds and whether it is susceptible to these attacks. DAST is a valuable component of the DevSecOps approach in robotics development [P24]. By incorporating DAST into the testing phase, roboticists can gain insights into the security vulnerabilities of their applications from an external perspective. This helps in identifying and addressing potential security risks, ensuring the development of more secure and resilient robotics systems [P24].
5. **Threat Modelling tool:** A threat modeling tool is a software application or framework that helps in the process of threat modeling. It is a systematic approach to identifying and assessing potential threats and vulnerabilities in a system or application [P08, P54, P24]. It helps in understanding the security risks and

making informed decisions to mitigate those risks [P51]. Threat modeling encompasses the depiction of an attack surface at various levels such as network, infrastructure, application, and human attack surface, providing a deeper insight into the necessary protective measures for the application. OWASP Threat Dragon[3] is an open-source threat modeling tool developed by OWASP (Open Web Application Security Project). It supports the creation of threat models using the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) threat modeling methodology. It provides a user-friendly interface and allows for collaboration among team members.

6. **Secret Management tool:** A secret management tool is a software application or service that helps in securely storing, managing, and accessing sensitive information such as passwords, API keys, encryption keys, and other credentials. These tools provide a centralized and secure way to handle secrets, reducing the risk of unauthorized access and improving overall security. Secret Management tools are created to assist in the management of secrets and various security methods for handling secrets. In addition to securely handling secrets, it is recommended to utilize secret detection tools to verify that secrets are not inadvertently exposed in public repositories. Secret detection tools can perform scans in public repositories to identify any unauthorized disclosure of secrets.
7. **HashiCorp Vault**[4] is an open-source tool that provides secure secret management and data protection. It offers features like secret storage, dynamic secrets, encryption, access control, and auditing. Vault supports various authentication methods and integrates with different cloud providers and identity management systems.
8. **Runtime Application Self-Protections (RASP)** is a tool utilized for application security purposes, aiming to safeguard and observe the behavior and requests of an application [P08, P54]. Through the continuous monitoring of the application's operations, input, and output, RASP is capable of identifying and defending against potential threats targeting the application. It is important to note that RASP is integrated directly within the application itself.
9. **Intrusion Detection** and **Intrusion Prevention Systems (IDS/IPS)** are security tools utilized in infrastructure to oversee and thwart potential intrusions within computer and network settings [P29]. IDS functions by monitoring network and computer activities for suspicious behavior that could signify a security threat or an attack, subsequently notifying about any identified security breaches. IPS performs similar functions as IDS but additionally takes proactive measures to hinder attacks on the system. Intrusion detection systems (IDS) for IIoT often employ a combination of techniques such as anomaly detection, signature-based detection, and behavior analysis [P29, P15]. Anomaly detection involves identifying deviations from normal patterns of behavior, while signature-based detection relies on known patterns or signatures of known attacks. Behavior analysis involves monitoring the behavior of devices and users to detect suspicious activities [P29].

[3]https://owasp.org/www-project-threat-dragon/
[4]https://www.vaultproject.io/

TABLE 12. Security tools identified in DevSecOps with corresponding DevOps phase security practice used in industrial environment.

Security Tools	DevSecOps Phase	Papers
SAST	Code, Build, Test	[P01, P11, P16, P19, P24, P30, P34, P41, P42, P47, P51]
SCA	Build, Test	[P01, P24, P16, P39, P42, P51]
DAST	Test, Release, Operate	[P16, P24, P42, P47, P51]
IAST	Test, Release, Operate	[P16, P34, P41, P47, P51]
Threat Modelling	Plan	[P42, P16, P47,P24]
Secret Management	Deploy, Operate	[P16, P34, P41, P47]
RASP	Deploy/Operate, Monitor	[P16, P30, P34, P41, P47]
IaC	Build, Test, Deploy	[P16, P19, P30, P34. P41, P42]
IDS/IPS	Deploy/Operate, Monitor	[P11, P16, P24, P34]

TABLE 13. Security tools identified in DevSecOps, each matched with specific examples of tools used in industrial environment.

Security Tools	Tools	Papers
SAST	SonarQube, Brakeman, PVS-Studio, Veracode, Coverity, Hakiri, Checkmarx	[P11, P16, P30, P39, P42]
DAST	OWASP ZAP, Arachni Scanner, Vuls, Nmap, SQLMap, Gauntit	[P11, P16, P30, P39, P41]
IAST	Hdiv	[P16, P24, P41, P42]
RASP	Hdiv, AppSenor	[P16, P34. P41, P47]
Secret Management	Git Secrets, Blackbox, Hashicorp Vault, Transcrypt, Pinterest Knox, GitLeak, CyberArk Conjur, ThoughtWorks Talisman, Berglas, Docker Secrets, Trufflehog	[P16, P42, P11]
Threat Modelling	Microsoft Threat Modeling Tool, ThreatModeler, OWASP Threat Dragon, CAIRIS	[P11, P16, P42, P47]
IaC	Cloud Custodian, Dev-Sec.io, InSpec, Ansible-Lint, Puppet-Lint, Foodcritic, Serverspec, Oscap	[P05, P11, P42, P47]
IDS/IPS	Fail2Ban, Snort, Suricata, OSSEC	[P14, P16, P42, P47]

The following table presents the list of tools used in DevSecOps to provide security and safety in Industry 5.0.

2) OTHERS DevSecOps TOOLS

Other tools in the literature have proven their worth in information security in DevSecOps in Industry 5.0. Cankar et al. [16] propose the use of two tools, IaC Scan Runner and LOMOS, which work together to enhance security in the DevSecOps process. IaC Scan Runner is an open-source solution developed in Python that inspects various IaC languages during application design time. It helps identify potential flaws in the code, which is crucial for ensuring security in sensitive domains like healthcare and maritime applications. LOMOS is a run-time anomaly detection tool that uses log analysis and artificial intelligence. It complements the static analysis capabilities of IaC Scan Runner by monitoring the behavior of the application during run-time and detecting any abnormal activities that may indicate security breaches. The combination of these two tools provides a valuable contribution to the DevSecOps toolset, enabling developers to identify and address security vulnerabilities throughout the software development and service delivery process as suggested by Cankar et al. [16].

F. RQ6: ENSURING THE CONFIDENTIALITY, AVAILABILITY, AND INTEGRITY OF DATA IN INDUSTRY 5.0 WITH DEVSECOPS

In this section, Industrial IoT security are analyzed with a focus on their impact on the confidentiality, integrity, and availability of data and the countermeasures when using DevSecOps. To ensure the confidentiality, integrity, and availability of IoT data, it is important to consider the types of attacks that can occur.

1) IIoT ATTACKS

We have conducted a comprehensive mapping of all the attacks that were previously examined by researchers. The IIoT architecture typically consists of multiple layers that work together to enable connectivity, data collection, analysis, and control in industrial environments. The commonly recognized layers in the IIoT architecture are:

a) **Perception Layer:** The IIoT architecture is divided into different layers, and the first layer is the perception layer. This layer mainly consists of two components: the physical (PHY) layer and the medium access control (MAC) layer. The PHY layer is responsible for handling hardware components such as sensors and devices, which are used to transmit and receive information using various communication protocols [74] and [81]. Our research has identified potential attacks, including tampering, Sensor attacks, and Denial of Service (DoS) attacks. Tampering can occur through physical destruction, injection of malicious code, and jamming of nodes. DoS attacks could involve manipulating the physical connection etc. DDOS attacks occur most frequently [P49]

b) **Network Layer:** The network layer plays a vital role in IIoT systems as it facilitates transmission and redirection of data via various connection protocols such as GSM, LTA, WiFi, 3-5G, IPv6, IEEE 802.15.4, etc. These protocols connect devices to smart services [74], [81]. Based on our research, we have identified two primary types of attacks that can affect the network layer of the Industrial Internet of Things (IIoT), namely, Man-in-the-Middle (MITM) and Denial-of-Service (DoS) attacks. Moreover, the DoS attack can be executed through various methods, leading to the unavailability of network resources for their intended recipients [P49].

c) **Application Layer:** The application layer, which is the third layer in IIoT systems, provides services to users through mobile and web-based software [74], [81]. Various types of attacks often compromise the security of the IIoT application layer. There are mainly four categories of assaults that target the application layer of IIoT, namely sniffing, phishing, malicious code injection, and DoS [P49].

The following table shows the different attacks linked to the different layers of the Industrial Internet of Things. Upon analyzing the data provided in the table, it has been observed that Denial of Service (DoS) attacks are consistently highlighted as one of the most prevalent forms of attacks in the field of IIoT research.

TABLE 14. Security attacks on IIoT per layer.

Layer	Attack Name	Ref. Papers
Application		
	Denial of Service	[74], [81], [57]
	Cross-site scripting (XSS)	[82], [57], [73]
	Man in the Middle Attack	[82], [73], [57], [73]
	Sniffing Attack	[74], [81], [57], [73]
	Acces Control Attack	[81], [73], [57], [73]
	Malicious code injection Attack	[74], [57], [57], [73]
Network		
	Routing Attack	[74], [57], [82], [73]
	Stockage Attack	[74], [57]
	Exploit Attack	[82], [57]
	Man in the Middle Attack	[74], [73], [57]
	DDOS Attack	[74], [73], [82], [57]
	Phishing Attack	[82], [57]
Perception		
	Eavesdropping Attack	[81], [57]
	Malicious code Injection Attack	[57], [81]
	Node Capture Attack	[81]
	Side Channel Attack	[57]
	False Data Injection Attack	[81], [57]

Attack That Could Compromise the CIA: A Denial of Service (DoS) attack is a relatively simple attack that aims to disrupt the availability of a system. This type of attack is carried out by inundating the target with more network traffic than it can handle, which prevents it from responding to legitimate requests [57]. In IIoT environments, potential targets for a DoS attack are devices and network itself. This attack can cause significant network latency, which may impede communications.

Another attack that can compromise the security of the IIoT is a Man-in-the-middle (MITM) attack. This kind of cyber attack happens when a malicious actor intercepts the communication between two endpoints as described by Serror et al. [57], [74].

By positioning themselves between the endpoints, the attacker can secretly monitor the data being transmitted or even modify it while pretending to be one of the legitimate parties involved [16]. Packet injection occurs when a third party injects packets into a TCP stream, which can be harmful to communication as described by Serror et al. [57], [74].

A network intrusion is an attempt to harm the confidentiality, integrity, or availability of a host or network. It is one of the most frequent threats and can cause potential damage to the Industrial Internet of Things as presented by Sharghivand and Derakhshan [76].

Phishing Attacks: Phishing attacks are major security threats, involving impersonation and unauthorized access to sensitive information, it exhibits the most elevated likelihood of happening. *Code Injection:* Code injection is a security threat that DevOps teams should prevent. Attackers inject malicious code into an application to compromise the system or steal data, leading to data breaches and downtime.

2) SECURING IIoT WITH DEVSECOPS

DevSecOps is an approach that integrates security practices into the DevOps process to ensure that security is considered and implemented throughout the entire software development lifecycle. When it comes to IIoT attacks, the implementation of DevSecOps principles and practices becomes crucial to mitigate security risks and protect IIoT systems. We created a six-step workflow for DevSecOps in IIoT, which is depicted in Figure 8. The six steps include (1) Plan, (2) Code, (3) Build, (4) Test, (5) Deployment, and (6) Operation and Monitoring. In the following sections, we will discuss each step in detail.

1. **Plan Phase:** Based on studies [P08, P11, P54, P24, P51] during the Plan stage of DevSecOps, teams establish the initial roadmap for their project by defining project goals, requirements, and timelines. This involves activities such as gathering user stories, prioritizing features, and assigning tasks. During this phase, the team identifies project objectives and security needs. They engage in threat modeling to understand security vulnerabilities and plan security measures accordingly.

i) **Threat modeling**: Threat modeling is an engineering technique used to identify potential risks to an application and develop countermeasures to mitigate them, ultimately helping to minimize risk and meet security objectives [P08, P11, P54]. Threat modeling in IIoT is an iterative process that requires collaboration between different stakeholders, including system architects, security professionals, and domain experts. It helps organizations proactively identify and address security risks, ensuring the resilience and security of their IIoT deployments. In DevSecOps planning, threat modeling integrates security measures from the outset to proactively identify security concerns [P24, P51]. One widely recognized approach to threat modeling is the STRIDE framework. It was proposed by Howard and Lipner [P79] and categorizes threats into six main types: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege. Typically, STRIDE threat modeling is conducted by security experts in conjunction with developers, architects, and other stakeholders involved in the software development process. These collaborative efforts ensure that security considerations are integrated into DevOps planning throughout the development life cycle [P08, P11, P54]. Potential threats are identified, assessed, and mitigated at an early stage of development through this approach.

ii) **Impact Analysis:** Software impact analysis is a crucial process that analyzes, predicts, and estimates the potential consequences before a change in the deployed product [P24, P51, P93]. Impact analysis integrates security considerations into the planning phase of DevOps by analyzing potential unexpected side effects of decisions or changes within a system and identifying potentially affected areas [P08, P11, P54]. This process starts by identifying impacted modules and functionality, describing proposed changes, and delineating affected areas. Risk assessment is used to evaluate potential risks associated with each change, such as performance changes, security vulnerabilities, and compatibility issues, often using a qualitative scale or numerical scoring system [P24, P51].

2. **Code Phase:** In the current stage of DevSecOps, development teams create functionalities by using version control systems like Git to commit their code changes [P24, P51]. This helps in easy collaboration and tracking of changes. This step is an important part of the Continuous Integration/Continuous Deployment (CI/CD) pipeline. In CI, developers regularly integrate their work into the main branch of the version control system. On the other hand, CD automates the deployment of software changes to the production environment without requiring human intervention.

i) **Vulnerability Detection:**. Developers' source code can be scanned for potential vulnerabilities by using vulnerability detection (VD) techniques as the traditional static analysis methods [P24, P51]. Common approaches to vulnerability detection in IIoT include vulnerability scanning, penetration testing, code review, security audits, threat intelligence monitoring, firmware analysis, and implementing secure development practices [P49].

ii) **Vulnerability Classification:** Developers can analyze code for the potential types of vulnerabilities by examining the source code. Such analysis helps developers understand the detected vulnerable source code and provide them with useful insights. By utilizing this

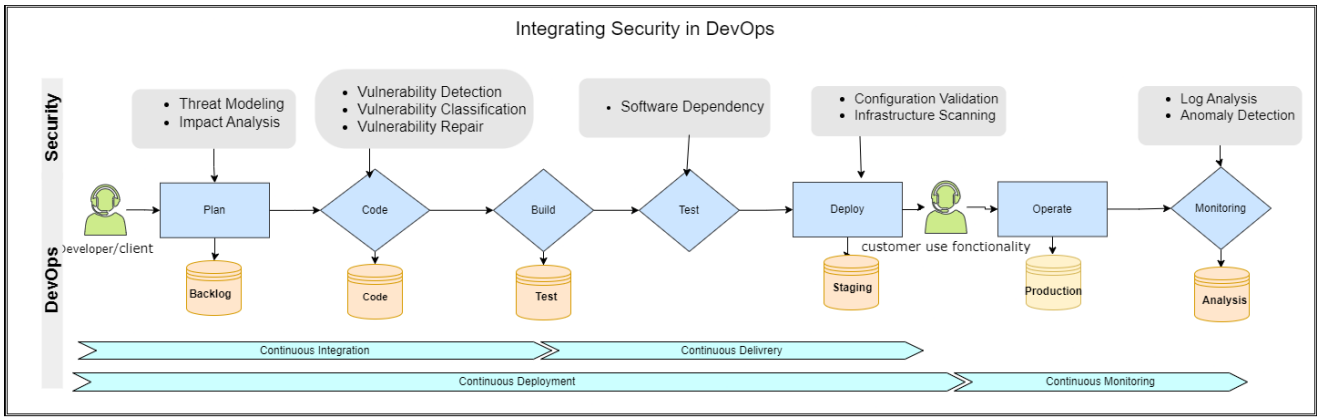

FIGURE 8. Integration of Security in DevOps Pipeline.

approach, developers can promptly prioritize resolving critical vulnerability types [P08, P11, P54]. Vulnerability classification in IIoT involves categorizing vulnerabilities based on their characteristics and impact on the system. Common classifications of vulnerabilities in IIoT include software vulnerabilities, network vulnerabilities, physical vulnerabilities, configuration vulnerabilities, supply chain vulnerabilities, and human vulnerabilities. These classifications help prioritize remediation efforts, allocate resources effectively, and implement appropriate security controls in IIoT systems [P49].

iii) **Vulnerability Repair:** New solutions are available that can automatically suggest fixes for buggy or vulnerable programs, eliminating the need for manual code repair which is time-consuming and labor-intensive. Vulnerability repair in IIoT involves addressing and fixing identified vulnerabilities in the system to enhance security and protect against potential attacks [P49]. The repair process typically includes applying patches and updates, making configuration changes, updating firmware, implementing security controls, following secure coding practices, conducting regular vulnerability assessments, and establishing an incident response plan. It is an ongoing process that requires continuous monitoring, testing, and staying updated on emerging threats [P49].

3. **Build, and Test Phase:** During the Build and Test phase of the DevOps process, software code undergoes compilation and rigorous testing to ensure its functionality and reliability. Once the code has been validated, it is deployed to the production environment, customized, configured, and installed for end-users. This phase involves automating the deployment process to ensure consistency and reliability [P24, P51].

i) **Configuration validation:** Configuration validation is a crucial component of DevSecOps. It guarantees that the configurations of software systems, including parameters and settings, are precise, efficient, and secure. Misconfigurations can result in vulnerabilities and system failures, making strong validation procedures necessary for protecting software systems against potential threats [P08, P11, P54].

4. **Deployment Phase:**
Deployment phase in DevSecOps refers to the process of releasing and deploying software applications or updates into production environments. It involves activities such as packaging the application, configuring the deployment environment, and deploying the application to servers or cloud platforms. During the deployment phase, various factors can be challenging and may need to be considered to ensure a successful deployment. These factors can include:

i) **Infrastructure Scanning:**. In DevSecOps, Infrastructure Scanning is crucial for secure and compliant software systems. IaC tools like Ansible, Chef and Puppet automate and scale infrastructure provisioning and configuration. They allow defining infrastructure configurations as machine-readable code, enabling consistent, repeatable deployments across environments [32]. IaC development can introduce security risks like hard-coded passwords [P24, P51]. The validated code is then deployed to production, requiring customization, configuration, and installation for end-user access [P08, P11, P54].

5. **Operation and Monitoring Phase:**. In the Operation and Monitoring phase of DevOps, the focus is on maintaining and monitoring the deployed software for optimal performance and security. The phase involves leveraging actionable intelligence and data-driven, event-driven processes to identify, evaluate, and respond to potential risks promptly [P08, P11, P54].

i) **Log Analysis:** Organizations use AI techniques to effectively detect and mitigate anomalies in system logs, enhancing system reliability with data from application logs and runtime environments [P18]. Log analysis plays a crucial role in identifying and mitigating security threats in IIoT (Industrial Internet of Things)

environments. By analyzing logs generated by various devices, systems, and applications within the IIoT ecosystem, organizations can gain insights into potential security incidents, anomalies, and vulnerabilities.

ii) **Anomaly Detection:** Anomaly detection in IIoT involves identifying patterns or behaviors that deviate significantly from expected behavior [P24, P51].

V. RELATED WORK

We are not the first ones to realize the study of DevOps and security DevOps challenges in the realm of the IIoT. Various studies have been issued that delve into different facets of DevOps and DevSecOps in IIoT. These can be broadly grouped into analyses of existing literature regarding challenges and prerequisites, the growing level of DevOps and DevSecOps within the IIoT, and the security ramifications of industrial operations. Hereafter, we provide a concise overview of recent relevant research categorized in this manner and elucidate how our study supplements and expands upon the current state of knowledge in the field.

A. DevOps AND DevSecOps APPLIED IN THE CONTEXT OF INDUSTRY 5.0

Several studies have been carried out in the literature on DevOps that presented challenges and solutions to introduce Industry 5.0 in industrial production environments.

Blüher et al. [14]explore the application of DevOps in the industrial context, particularly in series manufacturing, the principles, and culture of agile software development in the context of DevOps. It outlines the steps to create and validate the DevOps concept. It discusses the benefits of its implementation and the conditions under which DevOps can also be used in the industrial context of series manufacturing to steadily develop and provide software features used in these environments (e.g., for monitoring and maintaining manufacturing machines). Khan et al. [38] explore and discuss challenges related to DevOps culture and practices, and investigate the cultural challenges organizations face when implementing DevOps, a set of practices, and a cultural movement that aims to break down barriers between development and operation teams. Hasselbring et al. [31], [33] presented Industrial DevOps as an approach that helps in introducing DevOps methods and culture into industrial production environments. This approach enables the interconnection of stakeholders, systems, and data through incremental steps. Titan is a software platform that supports the Industrial DevOps approach. It helps to integrate production environments with Industrial DevOps and addresses specific challenges such as energy management and predictive maintenance, and in [33] discussed the Titan Control Center a software platform that supports research on industrial big data analytics, which analyzes and visualizes data streams from Internet of Things sensors in industrial production and performs different types of aggregations, correlation, forecasting, and anomaly detection to provide deeper insights into industrial production data for enabling Industrial DevOps.

Demertzis et al. [21] present a comprehensive framework for the management and protection of industrial data in the context of Industry 5.0. This framework specifically addresses the requirement for effective handling and analysis of large volumes of data in Industry 4.0, which involves the integration of CPS and AI. By combining contemporary software development techniques, the proposed framework aims to optimize and streamline the management of big data within an industrial ecosystem. Its primary objective is to bridge the existing gaps in the handling and protection of industrial data, which is often characterized by a lack of interoperability. Moreover, the framework facilitates the prediction and evaluation of threat-related situations within an industrial ecosystem, all while upholding principles of privacy and confidentiality. Moyon et al. [55] present a systematic approach to integrate standard-based security activities into DevOps pipelines, highlight their automation potential, and evaluate a large industrial company considering the IEC 62443-4-1 security standard that regulates ICS. Morales et al. [53] propose a guide to implement DevSecOps in defense and highly regulated environments, including systems of systems. It outlines the dimensions of change required for adopting DevSecOps and introduces the principles, operations, and expected benefits of DevSecOps. It describes the objectives and activities needed to implement the DevSecOps ecosystem, including preparation, establishment, and management. It emphasizes the importance of preparation to establish achievable goals and expectations, as well as the establishment phase to evolve culture, automation, processes, and system architecture. Wang et al. [90] present an enterprise manufacturing archive management system and management method based on DevOps integration are presented, which consists of a manufacturing archive acquisition unit, an enterprise information acquisition unit and an archive authenticity comparison unit, which is used to compare manufacturing archive information with production detection data in the same production process.

Fu et al. [27] investigate CI failures in four large industrial projects and identify the distribution of different types of build failures in each of the four CI projects, concluding that configuration problems are a significant issue, as pipeline scripting and dependency errors make up many failures.

Dakkak et al. [19] propose a Controlled Continuous Deployment approach, which considers software-intensive embedded systems' constraints, such as high reliability and availability requirements, limited possibility for rollback after deployment, and the high volume of in-service systems in the market.

Antonino et al. [7] analyze traditional architecture evaluation methods and Industry 4.0 scenarios and propose an approach based on Digital Twins and simulations to continuously evaluate runtime quality aspects of the architecture and systems of industrial production plants.

Shahin and Babar [75] present An industrial case study that has empirically identified and synthesized the key architectural decisions essential to DevOps transformation by two software development teams. It reveals that, apart from the chosen architecture style, DevOps works best with modular architectures.

1) DevOps AND DevSecOps IN IIoT

IIoT applications often require custom software development to control and monitor industrial equipment. DevOps practices have been applied to the development and deployment of IIoT applications. DevOps and the IIoT need robust security practices. In IIoT, the security of industrial systems is critical to prevent potential risks and breaches. There is a lot of interest in applying DevSecops to the IIoT.

Bijwe and Shankar [10] identify challenges in implementing a DevOps culture in IoT applications, such as poor communication, lack of DevOps experts, weak collaboration, and limited management support. It emphasizes the importance of collaboration, sharing, efficiency, and quality as effectiveness measures in IoT projects. It proposes the Industrial DevOps Maturity Model (IDMM) as a solution to these challenges, providing guidelines for implementing DevOps in IIoT applications

Bahaa et al. [9] suggest practical strategies for detecting and mitigating IIoT attacks, including the use of machine learning techniques, hybrid frameworks, advanced monitoring infrastructure, and DevSecOps pipelines. These approaches can enhance the security and resilience of IIoT systems in enterprises and the private sector.

Solayman and Qasha [78] examine the smooth incorporation of DevOps tools for the automation of provisioning in IoT applications across multiple infrastructures. They elucidate the necessity for automated provisioning and orchestration in IIoT ecosystems to augment the performance of the system. Paprzycki et al. [59] present an innovative methodology for the advancement of software platform development, utilizing the principles of DevOps and DevSecOps to facilitate the implementation of next-generation IoT deployments. They examine the various stages and layers within the architecture where DevSecOps may be implemented, while also emphasizing the advantages of this approach in facilitating continuous integration within software projects. Yasar and Teplov [93] explore the application of DevSecOps principles to software-intensive domains such as robotics and autonomous vehicles. To address the distinctive obstacles encountered in embedded systems, there is a need to modify existing DevSecOps frameworks. It underscores the significance of effective communication and collaboration among teams and stakeholders to attain DevSecOps in embedded systems. Additionally, the authors delve into the cultural hurdles associated with the development of embedded systems, such as the necessity for specialized module teams to engage in inter-team communication. Technical difficulties encompass the automation of deployment, testing, and the acquisition of post-production data. Moyón et al. [54]; Voggenreiter et al. [88] identified challenges in continuous secure software engineering, emphasizing the need for solutions that can be adopted on a scale, and proposed a methodology for automated management of security findings in industrial DevOps projects with impactful evaluation results. The integration of security standards into DevOps pipelines, with a specific emphasis on the IEC 62443-4-1 security standard for industrial control systems (ICS), is examined in the study conducted by Moyon et al. [55]. They pose a significant challenge due to the strict security regulations and standards that ICS must adhere to. The current body of research identifies gaps in the implementation of security standards in DevOps, particularly in the context of ICS. To address this, the study proposes a systematic approach that focuses on incorporating standard-based security activities into DevOps pipelines, with an emphasis on the potential for automation. To evaluate the effectiveness of this approach, it was applied within a large industrial company, taking into consideration the IEC 62443-4-1 security standard for ICS.

Zeller [95] highlights the challenges faced in developing safety-critical software-intensive systems in regulated domains from an industrial perspective. It proposes the concept of DevCertOps, which integrates software/system engineering and safety assurance life-cycle to achieve continuous safety assurance in safety-critical systems. Automation of the safety assurance process in the delivery pipeline is crucial for enabling the continuous delivery of software in safety-critical systems. The use of Model-Based Systems Engineering (MBSE) and model-based safety assurance concepts can help in the realization of continuous safety assurance in safety-critical systems.

Aljohani and Alqahtani [5] discuss the challenges in securing DevOps applications and introduce a unified framework for automating software security analysis in the DevSecOps paradigm. It emphasizes the lack of empowered automated security testing tools and proposes a framework approach to address these challenges.

VI. DISCUSSION

Industry 5.0 ecosystems are characterized by a higher degree of complexity compared to traditional software environments, stemming from the diversity of equipment, systems, and processes that require synchronization. This intricacy often presents challenges in the adoption of DevOps methodologies and tools.

Industrial enterprises typically exhibit a greater degree of hierarchical organization and compartmentalization in comparison to software enterprises. There often exists a divide within manufacturing companies between the teams specializing in Information Technology (IT) and Operation Technology (OT), as each team is assigned distinct responsibilities within the technology stack.

However, it was observed by organizations upon embracing the DevOps approach that security cannot be disregarded. This recognition led to the emergence of DevSecOps,

an approach that encompasses the inclusion of security in all stages of the software development lifecycle (SDLC). The adoption of DevSecOps practices has become crucial due to the constantly changing cyber threats.

Industry 5.0 is all about creating flexible industrial systems that offer better services, in less time, with higher quality and safety standards. However, software development needs frequent updates to ensure optimal quality and security. Real-time communication between development teams and consumers is also essential. Achieving this requires integration of information technologies, communication, and industrial technology.

Traditional methods are often expensive and lack adaptability. By building highly flexible manufacturing systems, companies can embrace Industry 5.0 and achieve digital transformation. To do so, the DevOps approach to software development is recommended. A robust security strategy is essential to tackle cyberattacks and vulnerabilities in the production line. The implementation of DevSecOps in Industry 5.0, particularly in the Industrial Internet of Things, helps mitigate specific security concerns. These include the potential for fatal consequences due to minor flaws in the adoption.

A. LIMITATION OF THE SYSTEMATIC MAPPING STUDY

The restriction to English-language studies may lead to the exclusion of pertinent research in other languages; however, English remains the predominant language for disseminating studies on this topic. Despite the valuable outcomes derived from this systematic mapping, they lay the foundation for a future iteration of the systematic mapping delineated in this study.

B. IMPORTANCE FOR FUTURE RESEARCH

The systematic mapping conducted in this study holds significant importance for researchers interested in exploring the realm of DevOps and DevsecOps, particularly focusing on its adoption in Industry 5.0 or the Industrial Internet of Things. This area of study is of particular interest to researchers due to its novelty and the limited amount of existing research. Researchers can leverage the advancements in this field to develop comprehensive guidelines for the effective adoption, implementation, and management of DevOps and DevSecOps practices in Industrial Internet of Things, thereby enhancing the current practices employed by companies in Industry 4.0 and solidifying good DevOps and DevSecOps practices. The advancements in this field will not only benefit researchers and Industries but also organizations at large. Many organizations have implemented DevOps and DevSecOps based on internal criteria without a thorough evaluation of the outcomes and benefits achieved.

VII. THREAT TO VALIDITY

In this section, we present the threats to the validity of our research and describe the measures we have implemented to address them. Threats to the validity of the results focus on issues that limit the ability to draw accurate conclusions. The threats to validity were based on the work and questions proposed by Petersen et al. [64]

A. CONSTRUCT VALIDITY

The construct validity of our study focuses on the operational measures used to represent the research objective and our approach to investigating these measures in the context of our research questions. Additionally, it incorporates the discernment of key research elements from the available literature. We conducted two rounds of snowballing to incorporate further research for evaluation. Ultimately, we established a rigorous set of inclusion and exclusion criteria to guarantee the inclusion of high-quality papers, restricting our selection to peer-reviewed journal and conference papers that demonstrated comprehensive and substantial findings [30].

B. INTERNAL VALIDITY

Internal validity refers to the errors and biases inherent in an experiment. We mitigate the internal validity threats by employing a meticulous strategy to ensure the internal validity of our findings. This approach entailed utilizing predefined keywords to conduct an extensive literature search and selecting and analyzing data through the application of thoroughly evaluated descriptive statistical methods on the gathered information, and subsequently applying a reverse snowballing process to the selected papers. We excluded any grey literature from our analysis [34].

C. EXTERNAL VALIDITY

External validity refers to the generalizability of our results. This study is limited to the academic search engines representing the academic DevOps and DevSecOps in Industry 4.0 search and focused on a limited number of peer-reviewed studies available in selected electronic databases [91].

D. CONCLUSION VALIDITY

Threats to conclusion validity are concerned with the factors that may hinder arriving at accurate findings, and these potential pitfalls were addressed by implementing the strategies proposed by Petersen et al. [64].

VIII. CONCLUSION

This work presents a Systematic Mapping Study (SMS) of DevOps and DevSecOps in Industry 5.0. It highlights the benefits, challenges, and security aspects of implementing DevOps and DevSecOps in Industry 5.0.

Through a comprehensive selection process, we identified 57 primary studies from a pool of 1,149 studies, which we then analyzed to address our six research questions.

The examination of DevOps and DevSecOps in Industry 5.0 has been a topic of current and increasing interest since 2019. Furthermore, it is acknowledged that this interest is widespread globally, particularly evident by the involvement of 16 countries across 3 regions (America, Europe, and Asia), which have collectively contributed to (80%) of the

studies. The DevSecOps approach to integrating security standards into DevOps pipelines has been validated in industrial environments. We have observed how the practices of the security standard fit into the DevOps pipeline. Similarly, 43 studies have been conducted within industrial environments (75%), while 25 have been performed in commercial environments (43%). Furthermore, 46 primary investigations (80%) have introduced tools designed to facilitate DevOps and DevSecOps in Industry 5.0.

The study demonstrates that it is feasible to apply successful software development practices that have already proven their worth in traditional settings to industrial production environments. It emphasizes the importance of embracing DevOps and DevSecOps for Industry 5.0, as it offers several advantages, including better dependability, faster development, efficient market launch, early feedback, and contextualized distribution methods.

However, IIoT and Industry 5.0 are currently in their early stages of development, with the anticipated disruptive changes still on the horizon. Thus, future studies need to focus not only on enhancing conventional security measures proposed by DevSecOps but also on introducing novel strategies to tackle the obstacles presented by the emerging IIoT. A notable area for exploration in this context is the utilization of technology blockchains, which provide an immutable and decentralized system of accountability across diverse scenarios.

A. FUTURE WORKS

We express optimism for the expansion of this field of research, alongside the increase in valuable contributions, to safeguard the integrity and confidentiality of IIoT systems. The prevalence of academic and collaborative efforts in IIoT security pattern research indicates the necessity for increased collaboration between academia and industry. This is particularly important given the burgeoning IIoT market, which necessitates practical and industry-oriented approaches. Therefore, it is evident that this field has yet to fully mature in both academic and industrial spheres. we identify two domains of research.

1) AI APPLIED IN DevOps AND DevSecOps

The integration of artificial intelligence and machine learning technologies into security solutions for the IIoT will have a notable impact on the improvement of DevSecOps practices by enhancing anomaly detection, behavior analysis, and threat prediction. Vemuri et al. [87] explore the integration of Deep Learning (DL) with DevOps methodologies to enhance predictive maintenance in the manufacturing industry. It introduces a comprehensive framework that combines data collection from diverse sources, preprocessing techniques, and appropriate DL models like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) for accurate predictions of equipment failures. The integration pipeline follows DevOps principles, including continuous integration, automated testing, and continuous deployment. Real-time monitoring and feedback mechanisms ensure model adaptability to evolving operational conditions.

Integrated AI into DevOps practices can be used to test, code, release, monitor, and improve the system. Through AI, the automation process delivered by DevOps can be improved efficiently. AI can be used to automatically check code for bugs, vulnerabilities, and deviations from coding standards. This development helps improve security and code integrity, minimizes human error, and reduces the need for manual reviews.

2) MACHINE LEARNING OPERATIONS IN INDUSTRY 5.0

Machine Learning Operations(MLOps), is a set of practices that involves applying DevOps principles to the machine learning lifecycle. Essentially, it involves collaboration among data scientists and other stakeholders to improve the speed and quality of model development. This is achieved through the monitoring, validation, and governance of machine learning models as presented by Kreuzberger et al. [40] Collaboration among data scientists is enabled, improving the speed, quality, and governance of model development through the monitoring and validation of machine learning models. There is growing scientific and business interest in the emerging field of MLOps, and a clear and standardized methodology is needed to conduct MLOps projects. Machine Learning Operations includes DevSecOps security practices to address the security risks of machine learning production systems. By integrating security into the Machine Learning Operations process, organizations can analyze the security risks of their ML-based systems, identify potential threats, and develop strategies to mitigate these risks. This ensures that machine learning systems are safe and secure from potential cyber attacks and security breaches, as presented by Bitton et al. [12].

REFERENCES

[1] M. Abbas, A. Hamayouni, M. H. Moghadam, M. Saadatmand, and P. E. Strandberg, "Making sense of failure logs in an industrial DevOps environment," in *Proc. Int. Conf. Inf. Technology-New Generat.* Cham, Switzerland: Springer, 2023, pp. 217–226.

[2] Z. Ahmed and Shoba. C. Francis, "Integrating security with DevSecOps: Techniques and challenges," in *Proc. Int. Conf. Digitization (ICD)*, Nov. 2019, pp. 178–182.

[3] M. A. Akbar, K. Smolander, S. Mahmood, and A. Alsanad, "Toward successful DevSecOps in software development organizations: A decision-making framework," *Inf. Softw. Technol.*, vol. 147, Jul. 2022, Art. no. 106894.

[4] M. Alawneh and I. M. Abbadi, "Expanding DevSecOps practices and clarifying the concepts within kubernetes ecosystem," in *Proc. 9th Int. Conf. Softw. Defined Syst. (SDS)*, Dec. 2022, pp. 1–7.

[5] M. A. Aljohani and S. S. Alqahtani, "A unified framework for automating software security analysis in DevSecOps," in *Proc. Int. Conf. Smart Comput. Appl. (ICSCA)*, Feb. 2023, pp. 1–6.

[6] R. Amaro, R. Pereira, and M. M. da Silva, "Capabilities and practices in DevOps: A multivocal literature review," *IEEE Trans. Softw. Eng.*, vol. 49, no. 2, pp. 883–901, Feb. 2023.

[7] P. O. Antonino, R. Capilla, R. Kazman, T. Kuhn, F. Schnicke, T. Treichel, A. Bachorek, Z. Müller-Zhang, and V. Salamanca, "Continuous engineering for Industry 4.0 architectures and systems," *Software, Pract. Exper.*, vol. 52, no. 10, pp. 2241–2262, Oct. 2022.

[8] S. Atif, "The role of Industry 4.0-enabled data-driven shared platform as an enabler of product-service system in the context of circular economy: A systematic literature review and future research directions," *Bus. Strategy Develop.*, vol. 6, no. 3, pp. 275–295, Sep. 2023.

[9] A. Bahaa, A. Abdelaziz, A. Sayed, L. Elfangary, and H. Fahmy, "Monitoring real time security attacks for IoT systems using DevSecOps: A systematic literature review," *Information*, vol. 12, no. 4, p. 154, Apr. 2021.

[10] A. Bijwe and P. Shankar, "Challenges of adopting DevOps culture on the Internet of Things applications—A solution model," in *Proc. 2nd Int. Conf. Technol. Advancements Comput. Sci. (ICTACS)*, Oct. 2022, pp. 638–645.

[11] A. Bitaillou, B. Parrein, and G. Andrieux, "Synthèse sur les protocoles de communication pour l'Internet des objets de l'industrie 4.0," Ph.D. thesis, Dept. Laboratoire Sci. Numérique Nantes, Institut d'Electronique Télécommunications Rennes, Université Nantes, Nantes, France, 2019.

[12] R. Bitton, N. Maman, I. Singh, S. Momiyama, Y. Elovici, and A. Shabtai, "Evaluating the cybersecurity risk of real-world, machine learning production systems," *ACM Comput. Surv.*, vol. 55, no. 9, pp. 1–36, Sep. 2023.

[13] T. Blinova, D. Singh, N. Kaur, Y. Lakshmi Prasanna, and P. Acharya, "IoT-driven innovations: A case study experiment and implications for Industry 5.0," *BIO Web Conf.*, vol. 86, Jan. 2024, Art. no. 01071.

[14] T. Blüher, D. Maelzer, J. Harrendorf, and R. Stark, "DevOps for manufacturing systems: Speeding up software development," *Proc. Design Soc.*, vol. 3, pp. 1475–1484, Jul. 2023.

[15] R. Brasoveanu, Y. Karabulut, and I. Pashchenko, "Security maturity self-assessment framework for software development lifecycle," in *Proc. 17th Int. Conf. Availability, Rel. Secur.*, Aug. 2022, pp. 1–8.

[16] M. Cankar, N. Petrovic, J. P. Costa, A. Cernivec, J. Antic, T. Martincic, and D. Stepec, "Security in DevSecOps: Applying tools and machine learning to verification and monitoring steps," in *Proc. Companion ACM/SPEC Int. Conf. Perform. Eng.*, Apr. 2023, pp. 201–205.

[17] T. Chen and H. Suo, "Design and practice of DevOps platform via cloud native technology," in *Proc. IEEE 13th Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Oct. 2022, pp. 297–300.

[18] A. Dagnino, M. Kolomycki, and A. Kucheria, "MAP: Design, development, deployment, and maintenance of industrie 4.0 AI applications," in *Proc. IEEE 8th Int. Conf. Big Data Comput. Service Appl. (BigDataService)*, Aug. 2022, pp. 108–113.

[19] A. Dakkak, J. Bosch, and H. H. Olsson, "Controlled continuous deployment: A case study from the telecommunications domain," in *Proc. Int. Conf. Softw. Syst. Processes Int. Conf. Global Softw. Eng.*, May 2022, pp. 24–33.

[20] L. de Aguiar Monteiro, D. S. M. P. Monteiro, W. H. C. Almeida, A. C. de Lima, and I. S. Sette, "Methods of implementation, maturity models and definition of roles in DevOps frameworks: A systematic mapping," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2020, pp. 1766–1773.

[21] K. Demertzis, L. Iliadis, E. Pimenidis, N. Tziritas, M. Koziri, and P. Kikiras, "Blockchained adaptive federated auto metalearning bigdata and DevOps cybersecurity architecture in Industry 4.0," in *Proc. Int. Conf. Eng. Appl. Neural Netw.* Cham, Switzerland: Springer, 2021, pp. 345–363.

[22] N. Chavan, N. Bharambe, S. Deshmukh, D. Ahire, and P. A. R. Jain, "Implementing DevSecOps pipeline for an enterprise organization," *Int. J. Adv. Res. Sci., Commun. Technol.*, vol. 2, no. 4, pp. 46–72, May 2022.

[23] J. Díaz, J. E. Pérez, M. A. Lopez-Peña, G. A. Mena, and A. Yagüe, "Self-service cybersecurity monitoring as enabler for DevSecOps," *IEEE Access*, vol. 7, pp. 100283–100295, 2019.

[24] O. Elijah, P. A. Ling, S. K. A. Rahim, T. K. Geok, A. Arsad, E. A. Kadir, M. Abdurrahman, R. Junin, A. Agi, and M. Y. Abdulfatah, "A survey on Industry 4.0 for the oil and gas industry: Upstream sector," *IEEE Access*, vol. 9, pp. 144438–144468, 2021.

[25] L. Faubel, K. Schmid, and H. Eichelberger, "Is MLOps different in Industry 4.0? General and specific challenges," in *Proc. 3rd Int. Conf. Innov. Intell. Ind. Prod. Logistics*, 2022, pp. 161–167.

[26] N. Ferry and P. H. Nguyen, "Towards model-based continuous deployment of secure IoT systems," in *Proc. ACM/IEEE 22nd Int. Conf. Model Driven Eng. Lang. Syst. Companion (MODELS-C)*, Sep. 2019, pp. 613–618.

[27] H. Fu, S. Eldh, K. Wiklund, A. Ermedahl, and C. Artho, "Prevalence of continuous integration failures in industrial systems with hardware-in-the-loop testing," in *Proc. IEEE Int. Symp. Softw. Rel. Eng. Workshops (ISSREW)*, Oct. 2022, pp. 61–66.

[28] S. Gupta, S. Modgil, B. Bhushan, U. Sivarajah, and S. Banerjee, "Design and implementation of an IIoT driven information system: A case study," *Inf. Syst. Frontiers*, pp. 1–15, Nov. 2023.

[29] L. Georgeta Guseila, D.-V. Bratu, and S.-A. Moraru, "DevOps transformation for multi-cloud IoT applications," in *Proc. Int. Conf. Sens. Instrum. IoT Era (ISSI)*, Aug. 2019, pp. 1–6.

[30] A. Haghighatkhah, A. Banijamali, O.-P. Pakanen, M. Oivo, and P. Kuvaja, "Automotive software engineering: A systematic mapping study," *J. Syst. Softw.*, vol. 128, pp. 25–55, Jun. 2017.

[31] W. Hasselbring, S. Henning, B. Latte, A. Möbius, T. Richter, S. Schalk, and M. Wojcieszak, "Industrial DevOps," in *Proc. IEEE Int. Conf. Softw. Archit. Companion (ICSA-C)*, Mar. 2019, pp. 123–126.

[32] C. Hegedus, P. Varga, and A. Frankó, "A DevOps approach for cyber-physical system-of-systems engineering through arrowhead," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, May 2021, pp. 902–907.

[33] S. Henning and W. Hasselbring, "The Titan control center for industrial DevOps analytics research," *Softw. Impacts*, vol. 7, Feb. 2021, Art. no. 100050.

[34] S. Jalali and C. Wohlin, "Agile practices in global software engineering—A systematic map," in *Proc. 5th IEEE Int. Conf. Global Softw. Eng.*, Aug. 2010, pp. 45–54.

[35] J. A. V. M. K. Jayakody and W. M. J. I. Wijayanayake, "Critical success factors for DevOps adoption in information systems development," *Int. J. Inf. Syst. Project Manage.*, vol. 11, no. 3, pp. 60–82, Oct. 2023.

[36] S. Keele, "Guidelines for performing systematic literature reviews in software engineering," Dept. Comput. Sci., Keele Univ., Keele, U.K., Tech. Rep. EBSE-2007-01, version 2.3, 2007.

[37] H. Khalid, S. J. Hashim, S. Ahmad, F. Hashim, and M. A. Chaudary, "Cybersecurity in Industry 4.0 context: Background, issues, and future directions," in *The Nine Pillars of Technologies for Industry 4.0*, vol. 4. Edison, NJ, USA: IET, 2020, pp. 263–307.

[38] M. S. Khan, A. W. Khan, F. Khan, M. A. Khan, and T. K. Whangbo, "Critical challenges to adopt DevOps culture in software organizations: A systematic review," *IEEE Access*, vol. 10, pp. 14339–14349, 2022.

[39] I. Koren, F. Rinker, K. Meixner, J. Matevska, and J. Walter, "Challenges and opportunities of DevOps in cyber-physical production systems engineering," in *Proc. IEEE 6th Int. Conf. Ind. Cyber-Physical Syst. (ICPS)*, May 2023, pp. 1–6.

[40] D. Kreuzberger, N. Kühl, and S. Hirschl, "Machine learning operations (MLOps): Overview, definition, and architecture," *IEEE Access*, vol. 11, pp. 31866–31879, 2023.

[41] M. Y. S. Krishna and S. K. Gawre, "MLOps for enhancing the accuracy of machine learning models using DevOps, continuous integration, and continuous deployment," *Res. Rep. Comput. Sci.*, pp. 97–103, Jun. 2023.

[42] P. Laihonen and T. Keränen, "Adoption of DevOps practices in the Finnish software industry: An empirical study," M.S. thesis, Dept. Sci. Technol., Aalto Univ., Espoo, Finland, 2018.

[43] S. Lavirotte, G. Rocher, J.-Y. Tigli, and T. Gonnin, "IoT-based systems actuation conflicts management towards DevOps: A systematic mapping study," in *Proc. 5th Int. Conf. Internet Things, Big Data Secur.*, 2020, pp. 227–234.

[44] M. F. Lie, M. Sánchez-Gordón, and R. Colomo-Palacios, "DevOps in an ISO 13485 regulated environment: A multivocal literature review," in *Proc. 14th ACM/IEEE Int. Symp. Empirical Softw. Eng. Meas. (ESEM)*, Oct. 2020, pp. 1–11.

[45] L. E. Lwakatare, I. Crnkovic, and J. Bosch, "DevOps for AI—Challenges in development of AI-enabled applications," in *Proc. Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM)*, Sep. 2020, pp. 1–6.

[46] R. C. L'Esteve, "Applying DevOps," in *The Cloud Leader's Handbook: Strategically Innovate, Transform, and Scale Organizations*. Berkeley, CA, USA: Springer, 2023, pp. 105–122.

[47] R. W. Macarthy and J. M. Bass, "An empirical taxonomy of DevOps in practice," in *Proc. 46th Euromicro Conf. Softw. Eng. Adv. Appl. (SEAA)*, Aug. 2020, pp. 221–228.

[48] P. K. Malik, R. Sharma, R. Singh, A. Gehlot, S. C. Satapathy, W. S. Alnumay, D. Pelusi, U. Ghosh, and J. Nayak, "Industrial Internet of Things and its applications in Industry 4.0: State of the art," *Comput. Commun.*, vol. 166, pp. 125–139, Jan. 2021.

[49] R. Mao, H. Zhang, Q. Dai, H. Huang, G. Rong, H. Shen, L. Chen, and K. Lu, "Preliminary findings about DevSecOps from grey literature," in *Proc. IEEE 20th Int. Conf. Softw. Qual., Rel. Secur. (QRS)*, Dec. 2020, pp. 450–457.

[50] V. Mayoral-Vilches, N. García-Maestro, M. Towers, and E. Gil-Uriarte, "DevSecOps in robotics," 2020, *arXiv:2003.10402*.

[51] I. Mizutani, G. Ramanathan, and S. Mayer, "Integrating multi-disciplinary offline and online engineering in industrial cyber-physical systems through DevOps," in *Proc. 11th Int. Conf. Internet Things*, Nov. 2021, pp. 40–47.

[52] J. Morales, R. Turner, S. Miller, P. Capell, P. Place, and D. J. Shepard, "Guide to implementing DevSecOps for a system of systems in highly regulated environments," Carnegie Mellon Univ., Softw. Eng. Inst., Tech. Rep. CMU/SEI-2020-TR-002, 2020.

[53] J. A. Morales, T. P. Scanlon, A. Volkmann, J. Yankel, and H. Yasar, "Security impacts of sub-optimal DevSecOps implementations in a highly regulated environment," in *Proc. 15th Int. Conf. Availability, Rel. Secur.*, Aug. 2020, pp. 1–8.

[54] F. Moyón, F. Angermeir, and D. Mendez, "Industrial challenges in secure continuous development," 2024, *arXiv:2401.06529*.

[55] F. Moyón, R. Soares, M. Pinto-Albuquerque, D. Mendez, and K. Beckers, "Integration of security standards in DevOps pipelines: An industry case study," in *Proc. 21st Int. Conf. Product-Focused Softw. Process Improvement*, Turin, Italy. Cham, Switzerland: Springer, Nov. 2020, pp. 434–452.

[56] T. Myklebust, M. A. Lundteigen, L. Bodsberg, and G. K. Hanssen, "Remote and agile improvement of industrial control and safety systems processes," in *Proc. 30th Eur. Saf. Rel. Conf. 15th Probabilistic Saf. Assessment Manage. Conf.*, 2020.

[57] A. C. Panchal, V. M. Khadse, and P. N. Mahalle, "Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures," in *Proc. IEEE Global Conf. Wireless Comput. Netw. (GCWCN)*, Nov. 2018, pp. 124–130.

[58] B. Pando and A. A. Dávila, "A systematic mapping study on software testing in the DevOps context," *Cyberleninka*, vol. 35, no. 1, pp. 163–188, 2023.

[59] M. Paprzycki, M. Ganzha, K. Wasielewska, and P. Lewandowski, "DevSecOps methodology for NG-IoT ecosystem development lifecycle—ASSIST-IoT perspective," *J. Comput. Sci. Cybern.*, vol. 37, no. 3, pp. 321–337, Sep. 2021.

[60] N. Paternoster, C. Giardino, M. Unterkalmsteiner, T. Gorschek, and P. Abrahamsson, "Software development in startup companies: A systematic mapping study," *Inf. Softw. Technol.*, vol. 56, no. 10, pp. 1200–1218, Oct. 2014.

[61] I. M. Pereira, T. Carneiro, and E. Figueiredo, "A systematic review on the use of DevOps in Internet of Things software systems," in *Proc. 36th Annu. ACM Symp. Appl. Comput.*, Mar. 2021, pp. 1569–1571.

[62] I. M. Pereira, T. G. de Senna Carneiro, and E. Figueiredo, "Understanding the context of IoT software systems in DevOps," in *Proc. IEEE/ACM 3rd Int. Workshop Softw. Eng. Res. Practices IoT (SERP4IoT)*, Jun. 2021, pp. 13–20.

[63] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," in *Proc. Electron. Workshops Comput.*, Jun. 2008.

[64] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Inf. Softw. Technol.*, vol. 64, pp. 1–18, Aug. 2015.

[65] A. Rahman, R. Mahdavi-Hezaveh, and L. Williams, "A systematic mapping study of infrastructure as code research," *Inf. Softw. Technol.*, vol. 108, pp. 65–77, Apr. 2019.

[66] R. N. Rajapakse, M. Zahedi, M. A. Babar, and H. Shen, "Challenges and solutions when adopting DevSecOps: A systematic review," *Inf. Softw. Technol.*, vol. 141, Jan. 2022, Art. no. 106700.

[67] R. N. Rajapakse, M. Zahedi, and M. A. Babar, "Collaborative application security testing for DevSecOps: An empirical analysis of challenges, best practices and tool support," 2022, *arXiv:2211.06953*.

[68] X. Ramaj, "A DevSecOps-enabled framework for risk management of critical infrastructures," in *Proc. IEEE/ACM 44th Int. Conf. Softw. Eng., Companion (ICSE-Companion)*, May 2022, pp. 242–244.

[69] X. Ramaj, M. Sánchez-Gordón, V. Gkioulos, S. Chockalingam, and R. Colomo-Palacios, "Holding on to compliance while adopting DevSecOps: An SLR," *Electronics*, vol. 11, no. 22, p. 3707, Nov. 2022.

[70] T. Rangnau, R. V. Buijtenen, F. Fransen, and F. Turkmen, "Continuous security testing: A case study on integrating dynamic security testing tools in CI/CD pipelines," in *Proc. IEEE 24th Int. Enterprise Distrib. Object Comput. Conf. (EDOC)*, Oct. 2020, pp. 145–154.

[71] V. Roblek, M. Meško, and A. Krapež, "A complex view of Industry 4.0," *SAGE Open*, vol. 6, no. 2, Apr. 2016, Art. no. 215824401665398.

[72] P. Abrahamsson, G. Botterweck, H. Ghanbari, M. G. Jaatun, P. Kettunen, T. J. Mikkonen, A. Mjeda, J. Münch, A. N. Duc, B. Russo, and X. Wang, "Towards a secure DevOps approach for cyber-physical systems: An industrial perspective," *Int. J. Syst. Softw. Secur. Protection*, vol. 11, no. 2, pp. 38–57, Jul. 2020.

[73] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102481.

[74] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and opportunities in securing the industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 17, no. 5, pp. 2985–2996, May 2021.

[75] M. Shahin and M. A. Babar, "On the role of software architecture in DevOps transformation: An industrial case study," in *Proc. Int. Conf. Softw. Syst. Processes*, Jun. 2020, pp. 175–184.

[76] N. Sharghivand and F. Derakhshan, "Data security and privacy in industrial IoT," in *AI-Enabled Threat Detection and Security Analysis for Industrial IoT*. Cham, Switzerland: Springer, 2021, pp. 21–39.

[77] M. Shaw, "Writing good software engineering research papers," in *Proc. 25th Int. Conf. Softw. Eng., Proceedings.*, 2003, pp. 726–736.

[78] H. E. Solayman and R. P. Qasha, "Seamless integration of DevOps tools for provisioning automation of the IoT application on multi-infrastructures," in *Proc. 3rd Int. Conf. Intell. Commun. Comput. Techn. (ICCT)*, Jan. 2023, pp. 1–7.

[79] E. Suescún-Monsalve, C.-J. Pardo-Calvache, S.-A. Rojas-Muñoz, and A. Velásquez-Uribe, "DevOps in Industry 4.0: A systematic mapping," *Revista Facultad de Ingeniería*, vol. 30, no. 57, Jul. 2021, Art. no. e13314.

[80] E. Suescún-Monsalve, C.-J. Pardo-Calvache, S.-A. Rojas-Muñoz, and A. Velásquez-Uribe, "Devops na indústria 4.0: Um mapeamento sistemático," *Revista Facultad de Ingeniería*, vol. 30, no. 57, 2021.

[81] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *J. Netw. Comput. Appl.*, vol. 161, Jul. 2020, Art. no. 102630.

[82] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2489–2520, 4th Quart., 2020.

[83] M. Trstenjak, M. Mustapić, P. Gregurić, and T. Opetuk, "Use of green Industry 5.0 technologies in logistics activities," *Tehnički Glasnik*, vol. 17, no. 3, pp. 471–477, Jul. 2023.

[84] I. Ungurean and N. C. Gaitan, "A software architecture for the industrial Internet of Things—A conceptual model," *Sensors*, vol. 20, no. 19, p. 5603, Sep. 2020.

[85] I. Ungurean and N. C. Gaitan, "Software architecture of a fog computing node for industrial Internet of Things," *Sensors*, vol. 21, no. 11, p. 3715, May 2021.

[86] M. Valentin, S. Patrick, and R. Eric, "Enhancing trust in Industry 4.0 traceability data using confidentiality-preserving digital ledger," in *Proc. 4th Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2022, pp. 33–36.

[87] N. Vemuri, V. Manoj Tatikonda, and N. Thaneeru, "Integrating deep learning with DevOps for enhanced predictive maintenance in the manufacturing industry," *Tuijin Jishu/Journal Propuls. Technol.*, vol. 43, no. 4, pp. 315–322, Jul. 2023.

[88] M. Voggenreiter, F. Angermeir, F. Moyón, U. Schöpp, and P. Bonvin, "Automated security findings management: A case study in industrial DevOps," 2024, *arXiv:2401.06602*.

[89] M. Voggenreiter and U. Schöpp, "Using a semantic knowledge base to improve the management of security reports in industrial DevOps projects," in *Proc. IEEE/ACM 44th Int. Conf. Softw. Eng., Softw. Eng. Pract. (ICSE-SEIP)*, May 2022, pp. 309–310.

[90] Z. Wang, M. Shi, and C. Li, "An intelligent DevOps platform research and design based on machine learning," in *Proc. 8th Int. Conf. Adv. Cloud Big Data (CBD)*, Dec. 2020, pp. 42–47.

[91] R. Wieringa, N. Maiden, N. Mead, and C. Rolland, "Requirements engineering paper classification and evaluation criteria: A proposal and a discussion," *Requirements Eng.*, vol. 11, no. 1, pp. 102–107, Mar. 2006.
[92] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proc. 18th Int. Conf. Eval. Assessment Softw. Eng.* New York, NY, USA: ACM, May 2014, pp. 1–10.
[93] H. Yasar and S. E. Teplov, "DevSecOps in embedded systems: An empirical study of past literature," in *Proc. 17th Int. Conf. Availability, Rel. Secur.*, Aug. 2022, pp. 1–6.
[94] S. Zaib and P. K. Lakshmisetty, "A systematical literature review and industrial survey in addressing the possible impacts with the continuous testing and delivery during DevOps transformation," M.S. thesis, Dept. Softw. Eng., Blekinge Inst. Technol., Karlskrona, Sweden, 2021.
[95] M. Zeller, "DevCertOps: Strategies to realize continuous delivery of safe software in regulated domain," in *Proc. IEEE/ACM 45th Int. Conf. Softw. Eng., Companion (ICSE-Companion)*, May 2023, pp. 334–335.
[96] X. Zhou, R. Mao, H. Zhang, Q. Dai, H. Huang, H. Shen, J. Li, and G. Rong, "Revisit security in the era of DevOps: An evidence-based inquiry into DevSecOps industry," *IET Softw.*, vol. 17, no. 4, pp. 435–454, Aug. 2023.
[97] C. Gan, J. Lin, D.-W. Huang, Q. Zhu, and L. Tian, "Advanced persistent threats and their defense methods in industrial Internet of Things: A survey," *Mathematics*, vol. 11, no. 14, p. 3115, 2023.
[98] W. M. van Bolhuis, R. Bernsteiner, M. Hall, and A. Fruhling, "Enhancing IoT project success through agile best practices," *ACM Trans. Internet Things*, vol. 4, no. 1, pp. 1–31, 2022.
[99] C. Ebert and L. Hochstein, "DevOps in practice," *IEEE Softw.*, vol. 40, no. 1, pp. 29–36, Jan./Feb. 2023.

KERSON BOISROND received the Graduate Diploma and master's degrees in software engineering from the University of Sherbrooke, Quebec City, Canada, where he is currently pursuing the Ph.D. degree in computer science. His doctoral research focuses on the security of software in industry 4.0. He has trained to publish in major refereed international conferences. His research interests include cybersecurity, AI, the IoT, DevOps, DevSecOps, the application of machine learning, data science, data analytics, and natural language processing.

PIERRE MARTIN TARDIF received the master's and Ph.D. degrees in electrical engineering from Laval University, Canada. He is currently a Professor with the School of Management, University of Sherbrooke. His research and academic expertise contribute to the field of management. His research interests include IT governance and cybersecurity. He plays a key role in a cybersecurity research collaboration between a team of professors from the University of Sherbrooke.

FEHMI JAAFAR received the Ph.D. degree from the Department of Computer Science, Montreal University, Canada. He was a Researcher with the Computer Research Institute of Montreal, an Adjunct Professor with Concordia University, Edmonton, and a Postdoctoral Research Fellow with Queen's University and Polytechnique Montreal. He is currently an Associate Professor with Quebec University at Chicoutimi and an Affiliate Professor with Laval University and Concordia University. His research has been published in top venues in computer sciences, including the *Journal of Empirical Software Engineering* (EMSE) and the *Journal of Software: Evolution and Process* (JSEP). He established externally funded research programs in collaboration with Defense Canada, Safety Canada, NSERC, and MITACS. His research interests include the security of the Internet of Things and the application of machine learning techniques in cybersecurity.