International Journal of Information Security (2025) 24:53
https://doi.org/10.1007/s10207-024-00951-8

REGULAR CONTRIBUTION

On the adoption and deployment of secure and privacy-preserving IIoT in smart manufacturing: a comprehensive guide with recent advances

Sani M. Abdullahi[1] · **Sanja Lazarova-Molnar**[1,2]

Accepted: 28 November 2024

Abstract
The adoption of the Internet of Things (IoT) in smart manufacturing has recently seen a boost in economic and technological advancement. This is attributed to improved operational efficiency resulting from streamlined interoperability, decreased downtime, and real-time processing as compared to conventional manufacturing industries. It also brings with it a massive deployment of intelligent systems and devices from both the Information Technology (IT) and Operational Technology (OT) realms within the Industrial IoT (IIoT) infrastructure, thus creating a heterogeneous interconnectivity. However, such inherent interconnectivity introduces significant security and privacy challenges. To mitigate these challenges, researchers and cybersecurity experts have recently proposed different defense mechanisms for the different facets of the cyber landscape within the IIoT infrastructure. Nevertheless, most of these techniques require major technical expertise to be implemented. Also, there is a lack of specific follow-through guides on how to adopt and implement such mechanisms. This paper aims to fill that gap by providing in-depth guidance on adopting and deploying different defense mechanisms designed to mitigate various cyber threats while ensuring secure and privacy-preserving IIoT infrastructure. The article first emphasizes the implications of cyber threats targeting IIoT tools and infrastructure as well as vulnerabilities emerging due to IT and OT convergence. It then delves into recent state-of-the-art protection mechanisms designed to mitigate these attacks based on a robust framework that includes all defenses. In addition, comprehensive guides to be adopted for a secure and privacy-preserving IIoT are provided. Finally, other challenges and open research questions are presented to pave the way towards efficient deployment of secure and privacy-preserving schemes for the IIoT in smart manufacturing.

Keywords Industrial internet of things · Smart manufacturing · Security and privacy · Adoption · Deployment

1 Introduction

The term "Industrial Internet of Things" refers to the interconnection of intelligent and networked industrial modules or clusters that are strategically deployed to optimize production and decrease operating expenditures through the implementation of continuous monitoring and effective management of industrial assets [1]. The global economic effect of this achievement has been significantly influenced by the widespread adoption of IoT across multiple industries, owing to its numerous advantages for industrial systems and platforms. Moreover, such expansion of the IoT is especially evident in the manufacturing sector due to the significant increase in global investment in IIoT platforms within the sector. It is projected that this investment will grow from USD 1.67 billion in 2018 to USD 12.44 billion by the year 2024 [2]. Additionally, it is worth mentioning that according to research conducted by the Information Technology and Innovation Foundation (ITIF) in collaboration with IoT analytics, the implementation of IoT infrastructure in the manufacturing sector has the potential to significantly improve performance and productivity by a range of 10% to 25% [3]. Furthermore, it is also projected that this technological advancement can facilitate the manufacturing of products amounting to around 1.8 trillion USD by the year 2025 [4] and a growth increase of over 24% from 2023 to 2030 [5]. These testify to the significant contribution of the IIoT in the manufacturing sector.

✉ Sani M. Abdullahi
saa@mmmi.sdu.dk

[1] Mærsk McKinney Møller Institute, University of Southern Denmark, Campusvej 55, 5230 Odense, Denmark

[2] Institute AIFB, Karlsruhe Institute of Technology, Kaiserstr. 89, 76133 Karlsruhe, Germany

Published online: 03 January 2025

Numerous manufacturing industry sectors are influenced by the IIoT through the integration of several technologies, such as big data analytics, AI, digital twins, machine learning, as well as cloud and edge computing architectures, in conjunction with the data used by these technologies to support industrial processes. However, cybersecurity concerns pose a significant obstacle to the adoption of IIoT, making it challenging to effectively utilize its capabilities. The implementation of IIoT systems significantly expands the potential for security breaches [6]. This is primarily attributed to the heterogenous integration of newly connected devices and technologies, which introduces novel security threats and renders the systems more susceptible to cyber intrusions. Consequently, the risks associated with IIoT systems encompass a broad range of implications, including the disruption or failure of control systems and processes, the illicit possession and acquisition of proprietary information, the compromise of sensitive data, the potential for industrial espionage, and many more.

When comparing the IIoT infrastructure to the conventional IoT model, it is evident that the former has a greater degree of sensitivity due to its larger size, increased complexity, enhanced robustness, and crucial ecosystem. Likewise, the susceptibility of IIoT to cyberthreats differs considerably from those experienced in the IoT across multiple aspects, such as threat surface, scalability, connectivity, interoperability, and the integration of OT. The typical IoT generally consists of regular IT infrastructure components, including workstations, servers, routers, and switches, which are considered part of their vulnerable attack surface. On the other hand, the IIoT broadens the potential for cyber-attacks by integrating a wide array of industrial equipment, such as control systems, cobots, sensors, actuators, and other field devices, along with different industrial protocols for communicating [7]. As such, the multitude of threats and risks associated with IoT tools, systems, and services are diverse and constantly evolving. The IIoT poses a significant risk to the safety, security, and privacy of individuals and systems, encompassing a broad range of potential threats. Therefore, it is crucial to identify all IIoT components that require protection and to formulate precise guidelines and security measures to safeguard these components from any form of cyber threats.

This survey provides robust defense mechanisms and comprehensive guidelines for a secure and privacy-preserving infrastructure for the IIoT in smart manufacturing. It highlights the security measures to be followed, protection mechanisms to be adopted and implemented, and privacy-preserving ethics for the IIoT that should be observed during the adoption and deployment phase of IIoT in smart manufacturing. The survey interacts with several regulations and policies, both in academia and industry, to deduce detailed procedures and protocols for a secure and privacy preserving IIoT. This is so that all future smart manufacturing systems can meet the required standards for secure and privacy-preserving infrastructure according to Industry 4.0. Further, we ensure that the provided guidelines, if adopted and deployed, will serve as a robust, secure-proof, and privacy-preserving foundation for the IIoT in smart manufacturing. These guidelines and protection mechanisms are also tailored towards ensuring the data privacy and security of the entire IIoT tools and infrastructure based on an in-depth look into the four-layered IIoT model framework described in Chapter 3.

Recently, different surveys have emerged regarding IIoT security. However, the majority of these surveys concentrate on specific security challenges within the IIoT or specific protection mechanisms, providing little to no guidance on how to adopt and implement various IIoT protection mechanisms while mitigating cyberthreats. This suggests the lack of comprehensive insights and guidance on how to adopt and deploy IIoT, especially in smart manufacturing. This, in turn, exacerbates the difficulties in guaranteeing the security of IIoT infrastructure. For instance, the surveys presented in [8, 9], and [2] primarily aimed to analyze the cybersecurity risks related to the growing smart manufacturing industry. In these surveys, authors evaluate the potential effects of these threats on the manufacturing sector and propose several strategies and methods to enhance the security in smart manufacturing without any specific follow-through guide on how to achieve this. Alabadi et al. [10] highlight numerous challenges, architectural requirements, and prospective future directions for IIoT. However, no guides are to be followed and implemented to secure the architecture from attacks. Franco et al. [11] provide a survey on the honeypots and honeynets for IoT, IIoT, and CPS. The authors identified various open issues without any guides on how to overcome them. Another recent survey by Wu et al. [12] delves into the management of network slicing and the application requirements of IIoT in smart factories. Challenges, open issues, future directions, as well as lessons learned, were all discussed without a tentative guide on how to implement the network slicing management for the IIoT architecture. Other surveys that highlight the cybersecurity challenges of IIoT in manufacturing include the works of [13, 14], and [15]. All of these surveys do not present concrete guidelines on ensuring the security of data, tools, and infrastructure within the IIoT. This observation signifies the need for a comprehensive survey that not only covers specific challenges and open issues but also implementation guides on how those challenges and issues can be mitigated.

To the best of our knowledge, this is the first survey that provides comprehensive guidelines and protection mechanisms for ensuring the security and privacy of IIoT for smart manufacturing. In this work, we first review existing relevant guides and regulations from both industry and academia, followed by an overview of the different attacks that IIoT tools

and infrastructure are susceptible to, as well as their protection mechanisms in terms of security and privacy. Next, we provide an overview of the comprehensive guidelines, which include measures and protocols to be followed during the adoption and deployment of IIoT tools and infrastructure. Finally, we discuss other possible countermeasures as well as challenges and open issues.

Our major contribution to this survey includes the following:

1. An in-depth study of the IIoT architecture, which aligns with the four-layered paradigm and encompasses all aspects of the IIoT, such as the different device components and communication protocols in the smart manufacturing domain, is provided.
2. Different attacks that pose a vulnerability to the adopted IIoT are analyzed, including possible threats that manifest due to IT/OT convergence. Countermeasures based on robust defense mechanisms are also provided through a comprehensive assessment of the IIoT model.
3. Guidelines for ensuring the security and privacy of the IIoT tools and infrastructure are covered in accordance with the adopted protection mechanisms. Most importantly, these guidelines capture both IT and OT aspects of the IIoT while ensuring that all defined security and privacy-preserving mechanisms are adopted and implemented accordingly.
4. In addition, the recent defense mechanisms are thoroughly discussed based on their novelty, contributions, and weaknesses. This will provide adequate insight to future IIoT security researchers on the best security and privacy measures to adopt and deploy.
5. Finally, other possible countermeasures as well as challenges and open issues that will aid future research are discussed.

The remaining parts of this paper are organized as follows: Sect. 2 gives a brief overview of existing guidelines in credible organizations and industry, as well as relevant guides and research works in academia. Section 3 delineates the smart manufacturing architecture within the IIoT, utilizing a four-layered model. This encompasses different tools, modules, and devices within the IIoT architecture that need to be protected against cyberattacks. Section 4 focuses on attacks and the defense mechanisms put in place to mitigate them. The chapter gives an insight into the different attacks that the adopted IIoT architecture can be vulnerable to, followed by the robust defense mechanisms that would be adopted and deployed to overcome such attacks. In Sect. 5, we focus on the main guides to ensuring the security and privacy of the IIoT tools and infrastructure in the manufacturing industry. These guides are given in consideration of the protection mechanisms adopted for IIoT security and privacy. In Sect. 6, other countermeasures as well as challenges and open research issues are given. Lastly, the conclusion is drawn in Sect. 7. Table 1 highlights the key contribution of our work compared to other survey papers in terms of the vulnerabilities and defense mechanisms covered.

2 Review of existing guidelines and best practices

To compile a comprehensive list of best guides and practices, as well as have a general overview of other protocols and see what will suit best for the IIoT infrastructure in smart manufacturing, this section analyzed different existing recommended security measures, keeping in mind the constant evolution of IoT infrastructures to meet Industry 4.0 requirements. Hence, the guides provide us with insight to identify what must be protected within the IIoT and to design suitable security protocols on how to prevent cyberattacks. This brings forth a brief review conducted in both academic and industrial settings, backed by the relevant government regulatory agencies.

Although there is currently no established comprehensive systematic framework for addressing security needs in the IIoT, the industry realized the need for standards in the early 2010s and subsequently proposed a number of recommendations. Since then, several guidelines and standards in the field of IIoT security and privacy provide manufacturers and users with guidance to improve security and privacy within the interconnected IIoT ecosystem. These guides have helped mitigate against several attacks that the IIoT are prone to, such as spoofing, spear phishing, malware, SQL injection, DDoS, etc. However, our exploration is mainly limited to the state-of-the-arts amongst these guides and standards, with consideration given to: The rapid development of the IIoT industry that may have rendered some ideas ineffective, though current studies regularly refer to and align with those of the past in crucial security domains. In addition to evaluating reports and articles, standard and best practices developed by credible associations such as NIST, ISO/IEC, and EU-ETSI or manufacturing bodies such as ENISA and CISA were assessed. All these were backed by government agencies to ensure full security and privacy compliance laid by the relevant authorities.

2.1 Survey of guides and regulations by credible organizations

2.1.1 National institute of standards and technology (NIST)

The US Department of Commerce's National Institute of Standards and Technology (NIST) published its first report

Table 1 Key contributions of our work over other survey papers in terms of IIoT vulnerabilities and defense mechanisms covered

Survey works	Vulnerabilities		Defense mechanisms							
	Different attacks	IT/OT threats	A	AC	DS	Network security			Data privacy	Guides
						RTM	NS	CS		
Mahesh et al. [8]	✓	×	✓	✓	✓	✓	×	✓	×	×
Phuyal et al. [9]	×	×	×	×	✓	×	×	×	×	×
Alabadi et al. [10]	×	×	×	×	✓	×	×	✓	×	×
Franco et al. [11]	✓	×	×	×	×	✓	✓	✓	✓	×
Wu et al. [12]	✓	×	×	×	×	✓	✓	✓	×	×
Shi et al. [13]	×	×	×	×	×	✓	✓	✓	×	×
Yu et al. [14]	✓	×	×	×	✓	✓	×	×	✓	×
Tange et al. [15]	×	×	×	×	×	✓	✓	✓	×	×
Mekala et al. [2]	✓	✓	✓	✓	✓	×	×	✓	×	×
Bravos et al. [16]	✓	×	✓	✓	✓	✓	×	✓	×	×
Panchal et al. [17]	✓	×	✓	✓	✓	✓	×	✓	×	×
Elhabashy et al. [18]	×	×	✓	✓	✓	×	×	✓	×	×
DeSmit et al. [19]	✓	×	×	×	×	×	×	×	✓	×
Chhetri et al. [20]	×	×	✓	✓	×	×	×	✓	×	×
Shah et al. [21]	✓	✓	×	×	×	×	×	×	×	×
Sezgin et al. [22]	✓	✓	×	×	×	×	×	×	✓	×
Jayalaxmi et al. [23]	✓	✓	✓	✓	✓	×	×	✓	×	×
Ours	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

A Authentication, *AC* Access control, *DS* Data security, *RTM* Real-time monitoring, *NS* Network segmentation, *CS* Cloud security

titled "IoT Device Cybersecurity Capability Core Baseline" (NIST IR 8259A) in 2020 [24]. The authors define a core baseline for the cybersecurity capabilities of an IoT device as a collection of device capabilities that are often required to facilitate overall cybersecurity measures aimed at protecting infrastructure, systems, and data. The recommended benchmark is the outcome of a collaborative endeavor aimed at developing a comprehensive inventory that reflects shared capabilities [24]. The document also outlines measures designed to boost the security of manufacturing industry and its products, thereby decreasing the number of IoT devices that have been compromised. Nevertheless, the guide fails to provide implementation procedures for these guidelines. However, the recently updated version of these guidelines (NIST IR CSF-2.0) [25] is focused on improving the implementation of cybersecurity in critical infrastructures. The framework proposed in the guide has been widely used to reduce cybersecurity threats in different manufacturing use cases.

2.1.2 European Union agency for network and information security (ENISA)

European Union Agency for Network and Information Security (ENISA) is another organization that has released numerous reports on the advancement of IoT security in industry. In 2017, the document "Baseline Security Recommendations for IoT" was published [26]. This project's objective was to acquire a deeper understanding of the security requirements of the IoT, with a particular emphasis on critical information services and infrastructure. The study offers an in-depth assessment of contemporary cybersecurity threats and an extensive set of protective measures for IoT devices. The authors compiled a list of recommendations, best practices, expert opinions, and industrial cyber security measures according to their findings. They further provide another guide specifically for securing the IoT [27]. The work encompasses a comprehensive compilation of additional IIoT security standards, which could count as an invaluable initial resource for further investigations. It also incorporates standards from a variety of sources, including the ISO/IEC.

2.1.3 European telecommunications standards institute (ETSI)

The European Telecommunications Standards Institute's (ETSI EN-303 645) guideline on cyber security for the consumer IoT is another important resource for securing IoT devices [28]. The document centers primarily on European regulations and seeks to establish an initial framework for IoT device production. It references several important projects, consisting of NIST and ENISA. In one of the initiatives, for example, it is striving to develop a framework to handle encrypted credentials in a complex setting of multifaceted devices. Consequently, manufacturers, executives, and experts rather than individual consumers are the intended audience. Recently, they also proposed an implementation guide for the consumer IO devices ETSI TR 103 621 [29]. The document provides guidelines to assist manufacturers and other relevant stakeholders in fulfilling the cyber security requirements established for Consumer Internet of Things (IoT) devices (ETSI EN-303) 645.

2.1.4 International organization for standardization/institute of electrotechnical commission (ISO/IEC)

The recently published International Organisation for Standardization/Institute of Electrotechnical Commission (ISO/IEC 27400:2022) document provides guidelines on risks, principles, and controls for the security and privacy of IoT solutions [30]. The document gives an in-depth analysis of risk sources for IoT systems while suggesting a plethora of security and privacy solutions to help mitigate any form of cyber threat. The document also provides best practice recommendations to facilitate compliance with GDPR by ensuring regulatory and legal adherence. One example of such a regulation is the EU Network and Information Systems Regulations (NISR), which provide legal measures (covered by D7.7) aimed at enhancing the overall security, encompassing cyber and physical aspects of information and network systems. Such systems play a crucial role in facilitating the accessibility of digital services ranging from data processing to data storage in the cloud. The growing importance of the internet and information systems as crucial facilitators of societal and economic development justifies the implementation of this measure.

2.1.5 Cybersecurity and infrastructure security agency (CISA)

As the sector-specific agency, the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS) collaborated with the Critical Manufacturing Sector Coordinating Council (SCC) to develop a sector-specific implementation guide centered on the manufacturing industry [31]. In line with NIST, CISA also provides a regulatory framework for information and cyber security guidance by evaluating and improving the ability of manufacturing industries to detect, prevent, and react to cyberattacks. It provides a high-level notion of risk management through the prioritize, orient, determine, analyze, and action plan concepts. The guide is a tool for harmonizing strategic operations and technological solutions for handling cybersecurity risks. It can be used to determine the most effective steps to mitigate a cyber threat. Organizations, industries, and businesses are just a few of the different categories of entities that can use the framework for various objectives.

The recommendations in the above-mentioned guides and standards are high-level, which might not be applicable to low-level systems, because no low-level system-specific information is included. To derive efficient security principles, it is essential to acquire thorough system understanding and analyze these recommendations within the context of this knowledge. In addition, substantial effort is required to verify these recommendations using structured tools, including the conversion of high-level suggestions into low-level security regulations and the design of such regulations for the security evaluation. Moreover, many of the proposed measures ought to have been proposed and implemented for large industries because they are beyond the user's control. However, to ensure the concerns on detection and prevention/mitigation are covered, our guides focus on low-level security regulations as well as the privacy threats related to the sharing of data in IIoT, which is discussed in Chapter 5.

2.2 Survey of guides and research works in academics

2.2.1 General surveys, guides, and research works

Despite reviewing various cybersecurity frameworks and guide recommendations from the perspective of credible organizations, it is crucial to also investigate academic works and see what they have to offer. This would provide us with an overview of the most effective security measures for the IIoT tools and infrastructure.

Given that most scholars acknowledge the fact that the majority of cyberattacks instigated against industrial systems lack preventive measures in place, it is crucial that preventive measures are considered prior to detection in the IIoT infrastructure. This will greatly help to minimize the likelihood of an attack. Some notable state-of-the-works in the literature that fulfil both the preventive and detective criterion includes following works:

In [16], Bravos et al. provide a detailed analysis of two tangible instances of connected IIoT systems in smart factory

and smart logistics environment, emphasizing the architectural decisions made to bolster cybersecurity measures. In addition, they include an interconnected industrial system that ensures safe data transmission and employs strategies for detecting and mitigating threats to both real-world data and IoT devices. Although the system is not readily available as a commercial product, its architectural design and outcomes demonstrate the benefits of employing advanced technologies like deep learning for threat detection and blockchain for improved communication within IIoT systems, specifically for the purpose of threat prevention. This analysis also explores the practical implementation of these technologies. The researchers ultimately presented the empirical findings pertaining to the different components of their system in the manufacturing domain, along with an evaluation of the overall system performance. Since the authors place significant emphasis on the independence and portability of various components within their system, the majority of these components may be readily modified and used as independent services within other systems. Also, the suggested architectural framework has the potential to be used in other emerging IIoT systems with little to moderate technical adjustments. Therefore, the findings of their study may serve as a baseline reference for future studies in this domain.

Mahesh et al. [8] conducts an analysis and evaluation of the cybersecurity vulnerabilities within the evolving digital manufacturing environment. They evaluate the potential threats based on different case study scenarios and consequences for the manufacturing sector and proposes effective strategies to safeguard manufacturing operations. In terms of attack prevention, the authors emphasize on the possibility that not all participants in a manufacturing industry have the same level of resources to implement the most sophisticated defenses, because the vulnerabilities inside for instance, a supply chain, in addition to jeopardizing their own resources, have the potential to compromise the assets of every party involved in the supply chain. Therefore, while their primary emphasis in the research was on the cybersecurity measures used in the manufacture of distinct components within a Digital Supply-chain Network (DSN), they also acknowledged the significance of other components within the DSN, including the information, financial, and commercial networks. Finally, they also suggest certain methods to be adopted to ensure threat mitigation, such as established information security techniques like data encryption, watermarking, and authentication.

In [32], the authors aimed to provide educational resources to those without specialized knowledge on the safe deployment of IoT devices. To accomplish this, a compilation of effective guides and methodologies has been furnished, derived from established frameworks. The execution of these security measures was shown in two distinct situations, using a range of network devices and taking into account the limits often encountered by SMEs. They also conducted an evaluation of the current vulnerabilities that exist in smart devices as well as the existing standards pertaining to the safe deployment of Internet of Things (IoT) devices. Next, they proceed to execute the prevailing optimal strategies for ensuring the security of interconnected network devices, with a specific emphasis on preventive measure to the issues posed by the IoT. Lastly, they laid the groundwork for presenting a pragmatic framework that facilitates the secure deployment of IoT devices within SMEs.

Recently, Mekala et al. [2] provided an extensive review of the Industrial Internet of Things (IIoT) framework by identifying distinct sectors in which IIoT adoption occurs, an evaluation of potential risks and vulnerabilities, and an in-depth analysis of countermeasures that are currently available. The authors also highlight some preventive measures based on the integration of different technologies such as edge, blockchain, and advanced artificial intelligence, including deep learning, machine learning, and big-data analytics, while bringing forth some future challenges that can be mitigated by such technologies, including maintaining scalability in the IIoT, effective resource management approaches that facilitate data transfer without modifying the computational storage capacity of the sensors, heterogeneity and diversity of IIoT applications and protocols, IIoT architecture design flaws, and mapping industrial applications against the threat environment.

According to [33], the plethora of security challenges faced by IoT require not just detective measures, but prevention should be at the forefront of mitigating cyberattacks. Therefore, the authors outlined several security needs that have been suggested for the IoT while providing a thorough categorization of the primary security concerns pertaining to the architecture of the IoT, taking into account the potential consequences of attacks and other emerging security concerns. Moreover, they systematically compile and visually represent the many countermeasures used to address these vulnerabilities, while considering recent advancements in security methodologies. In conclusion, an in-depth evaluation of the specified countermeasures for IoT security is undertaken.

2.2.2 Blockchain-based surveys and research works

Other works encourage the use of blockchain for secure smart factories; these include Elmamy et al. [34], Leng et al. [35], Rathee et al. [36], Maleh et al. [37], Pourrahmani et al. [38], Leng et al. [39], Nutter et al. [40], and Gimenez-Aguilar [41]. In [35], the authors examine the potential of blockchain systems for addressing cybersecurity challenges that may hinder the realization of intelligence in Industry 4.0. In this context, a total of eight cybersecurity concerns have been discovered within the realm of industrial systems. The authors then

created ten comprehensive metrics via a scrutiny of existing research on blockchain-secured smart manufacturing, with the aim of facilitating the implementation of blockchain applications in the production sector. They provide valuable insights that will guide future research directions in the field of blockchain-secured smart manufacturing which can possibly drive research efforts to address important cybersecurity challenges in order to achieve intelligence in the context of Industry 4.0. Despite the full trust in blockchain for ensuring the required protection against cyber threats, it still comes with its own fair share of vulnerabilities [42] such as the insertion of invalid transactions into a block, goldfinder, double spending, and wallet theft [42].

In another profound work by Nutter et al. [40], the authors identify major aspects of blockchain-based solutions in numerous sectors of Industry 4.0. In addition, they provided a framework that proved valuable in conceptualizing the integration of Industry 4.0 enabling technologies with blockchain technology, thereby facilitating the implementation of adept and effective blockchain-based solutions within the context of Industry 4.0. In conclusion, using the suggested framework, the authors propose a hypothesis about the progression of blockchain technology in Industry 4.0 environments while emphasizing the pertinent areas of study that scholars and professionals engaged in this domain should focus on in the immediate future.

In a rather unexpected approach, instead of focusing on proposing solutions and mitigation strategies against cyber threats, Rainmundo et al. [43] debate on security surrounding the current topics in IIoT. The authors argue that due to the need for decision-making, cybersecurity must first concentrate on the diverse vulnerabilities of IoT components before proceeding to work on its security mechanisms, such as access control, data storage, authorization, and privacy. While enterprises must adopt a cybersecurity plan with respect to their protection needs, emphasizing that organizations must stay abreast of technological advancements in order to respond appropriately to cybersecurity threats. In a nutshell, this all boils down to the fact that cyber security experts must be alert to the plethora of future challenges regarding cyber threats, while organizations must first look into preventive measures against cyber-attacks.

2.3 Chapter summary

This section provides a summary of conclusions derived from this chapter in relation to the crucial guidelines and security measures adopted for the benefit of the entire IOP tools and infrastructure. Below, we itemize our take from these surveys, both in academia and industry organizations.

Summary of Surveys from Organizations.

1. To ensure IIoT security, the majority of the guides emphasize adopting proactive security measures before detection (reactive) measures. As such, our guides also embrace this strategy, thereby making sure that proactive measures are taken into consideration for the security and privacy of the IIoT infrastructure.
2. Amongst the guides, ENISA and CISA can be applicable to organizations, industries, and businesses, depending on the framework scope and its various objectives. Therefore, IIoT security can derive advantages from the defined frameworks in these guidelines.
3. With the exception of ENISA and ETSI, other guides, especially NIST and ISO/IEC, are high-level, requiring an in-depth understanding of the infrastructure in order to analyze the measures within the context of the standards provided. Consequently, they might not be applicable to low-level industries.
4. ETSI is mainly concerned with the consumer aspect of the IIoT and focuses on European regulations. Its primary objective is to establish an initial framework for secure and efficient production within the context of consumer IoT. As such, some important benefits can be derived for the consumer side in the IIoT.
5. Most of the guides and regulations also provide a general overview of frameworks that can be used to determine the most effective steps to mitigate a cyber threat.

Summary of Survey works from Academia.

1. Fortunately, academia also places greater emphasis on proactive measures for ensuring IIoT security in the manufacturing industries prior to detection measures.
2. With the recent advances in deep learning and blockchain technologies, some of the works emphasizes the use of these advanced technologies for threat detection (via deep learning) and improved communication within IIoT systems (via blockchain). The adoption of such novel technologies shall be considered in our guides depending on the security, performance, and scalability tradeoffs.
3. In addition to ensuring the security of digital services, networks, data, the cloud, etc., some researchers emphasize adopting the right architectural framework in order to enhance the cybersecurity of the industry since the architecture encapsulates how services can be managed and how the network can be segmented, monitored, and mapped. This testifies to the need for adopting the right architecture for every IIoT.
4. For a more efficient integration of cybersecurity measures, independent implementation of each component within the IIoT is also encouraged. So do our guides for securing the entire IIoT infrastructure.
5. Other works emphasize that each component within the infrastructure should possess the same level of resources

to implement defenses because vulnerabilities within one component, such as a network, can lead to the compromise of other components, such as databases and devices. This is also captured in our guides.

6. Most research also stresses the potential of blockchain-based systems for addressing cybersecurity challenges that may impede the realization of intelligence in Industry 4.0. However, since the sole adoption of blockchain also comes with its fair share of vulnerabilities, ensuring a balance with other technologies is key for the optimal protection of the entire IIoT in our guides. Table 2 provides key contribution of our work over other existing security measures and regulations in terms of guidelines to be adopted and deployed in order to ensure the security and privacy of the entire IIoT ecosystem in smart manufacturing.

3 Architectural overview of IIoT

The conventional architecture of the IIoT for smart manufacturing encompasses the organization of digital networked systems in a manner that facilitates the establishment of network and data communication across various components, including IoT devices, actuators, data storage, etc. However, establishing a strong foundation for the IIoT is crucial for fostering a sustainable environment conducive to the long-term growth of IoT initiatives in smart manufacturing contexts. Also, the adoption of a process-oriented perspective on the IIoT recognizes that its implementation has a broader scope than the mere interconnection of various IIoT devices to the internet. As such, building a resilient infrastructure is a crucial component of ensuring the security and privacy of the entire IIoT. This section gives a detailed outline of the adopted architectural overview for smart manufacturing. It also describes all the relevant tools and devices that are involved in all operations within the IIoT infrastructure.

3.1 Framework and components of the IIoT architecture

The four-layered model, which delineates the standard design of an IIoT framework, has gained significant acceptance within the smart manufacturing industry [10]. The paradigm shown in Fig. 1 depicts the four distinct layers of a typical IIoT architecture, including the perception or devices layer, the network or gateway layer, processing or cloud layer, and the application or data management layer. Each layer encompasses various essential elements that helps with the functioning of the IIoT architecture. Below is the detailed description of each layer and its role in the IIoT.

1. *The perception or device layer*: The perception layer, often known as the device layer comprises a comprehensive array of devices such as actuators, robots, sensors, cameras, and other physical objects that are used for the purpose of data collection. The sensors used in the IIoT are often referred to as smart/intelligent sensors. One notable feature of intelligent sensors is their ability to establish communication with the network, usually by means of wireless signals as opposed to conventional cable industrial networks. In order to assure the reliable communication of accurate and real-time data by such intelligent sensors, the IEEE has derived standards and regulations in place [44]. Moreover, the sensors are also capable of gathering data from both the surrounding environment and the specific items they are tasked with monitoring. Subsequently, the acquired information is transformed into practical facts that individuals may effectively use. The actuators are responsible for controlling and adjusting the many processes that occur inside the measured area. The physical circumstances under which the data is created are modified. For instance, an actuator has the capability to either initiate the opening or closing of a valve or facilitate the movement of a robotic arm within the context of an autonomous assembling procedure.
   An additional essential characteristic of smart sensors is their capacity for self-identification and adaptability [45]. Thanks to the IEEE standard that is designed to create uniform identification criteria, enabling seamless interoperability among intelligent sensors produced by different manufacturers. This facilitates the efficient detection of crucial sensor data either in transit or at rest. Actuators and controllers are also recognized as integral components of this layer. In the realm of IIoT, controllers are often integrated into systems and designed to fulfill different roles.
2. *The network or gateway layer*: This layer comprises of specialized IIoT tools that facilitate the transmission of gathered data from the sensors and actuators. Here, the gateways are responsible for conducting local storage and processing of the gathered data before transmitting it to the subsequent tier in the IIoT infrastructure. It is essential to acknowledge that gateways are not designed for process management and only execute these activities on data prior to transmitting it to the cloud. As such, they can be considered as data-collection devices that remain integral components of the edge network. Based on the classification system, the gateways would still be categorized as edge devices. They also remain in close proximity to the sensors and actuators, where they perform data preprocessing at the edge.
   Nevertheless, substantial quantities of processed information need the use of considerable processing capacity,

Table 2 Key contribution of our work over other guides and survey papers in terms of guidelines to be adopted and deployed

Guides and Survey works	Guides to a secure and privacy preserving IIoT tools and infrastructures									
	Guide to secure digital services				Guide to secure network connectivity			Guide to secure cloud database	Guide to data privacy	
	A	AC	DS	T & DM	NS	NM	NC		PG-U	PG-I
NIST IR 8259A [24]	×	×	✓	✓	×	✓	×	×	×	×
NIST IR-CSF-2.0 [25]	✓	✓	✓	×	✓	✓	✓	✓	×	×
ENISA-Baseline [26]	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
ENISA-Secure IIoT [27]	✓	✓	✓	✓	✓	✓	×	✓	×	×
ETSI EN-303 645 [28]	✓	✓	✓	×	×	✓	×	✓	×	×
ETSI TR 103 621 [29]	✓	✓	✓	✓	✓	✓	×	✓	×	×
ISO/IEC-27400:2022 [30]	✓	✓	✓	✓	✓	✓	×	✓	✓	✓
CISA [31]	✓	✓	✓	✓	✓	✓	✓	✓	×	×
Our Guides	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

A Authentication, *AC* Access control, *DS* Data security, *T&DM* Tools and device management, *NS* Network segmentation, *NM* Network monitoring, *NC* Network configuration, *PG-U* Privacy guides for users, *PG-I* Privacy guides for industries

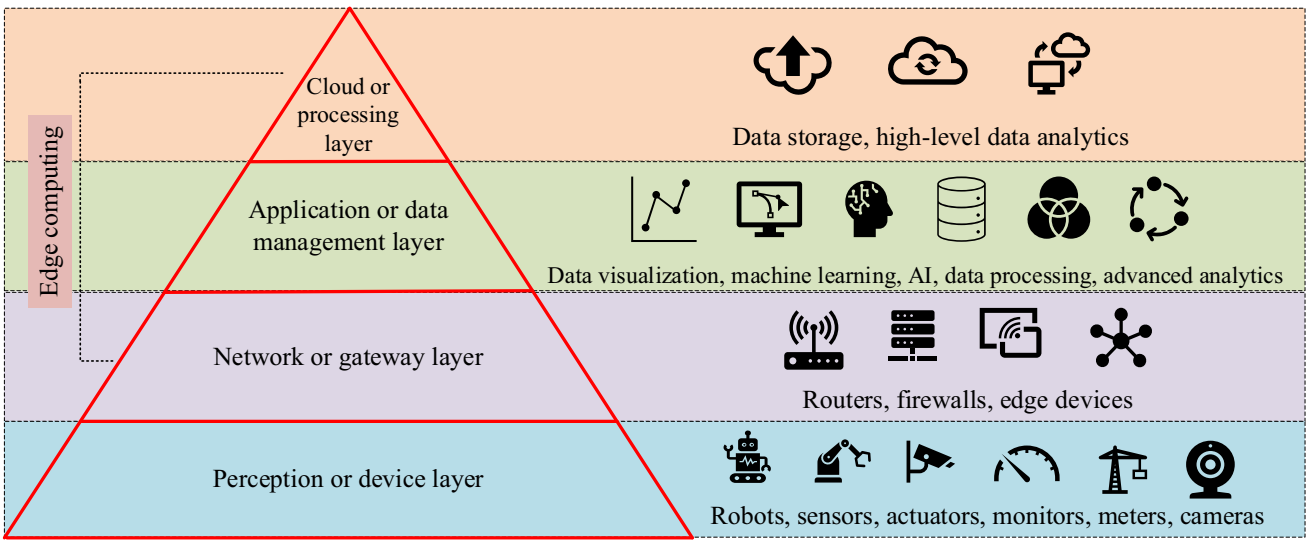

Fig. 1 The four distinct layers and components of a typical IIoT architecture

because the continuous data streaming generates substantial data flows that exceed the capacity for direct transmission to the cloud. The complexity of managing an IoT network increases significantly when there is a large number of sensors continuously transmitting data. Moreover, in the event that the sensor data is presented in analog format, it is necessary for the gateway to convert it into digital form in order to facilitate subsequent information processing [46].

3. *The application or data management layer*: After the collection of data, its conversion into digital format, and subsequent aggregation, the data is prepared for further processing using edge systems. The edge IT systems have the capability to be either onsite or remote; however, it is most often seen that these systems are located in close proximity to the sensors. This is the stage at which digitized and aggregated data is used for the purpose of conducting analytics. Furthermore, the available data exhibits coherence and logical consistency with the help of knowledge possessed via machine learning and data visualization. Once practical and implementable insight from the extracted data is gained, it is often followed by the insights acquired. The use of this supplementary processing mechanism effectively mitigates the volume of data being sent to data centers or cloud-based infrastructures. By adopting this approach, one is able to mitigate

problems related to downtime, storage, and security. In a nutshell, this layer entails the graphical user interfaces that aid in the interpretation of data derived from the preceding layers. In particular, user programs that are responsible for generating reports, performing analysis, and producing statistical data.

4. *The processing or cloud layer*: This layer encompasses the realm of cloud computing. Here, the data has been successfully sent to a database or server located inside a data center. Significant computational resources are often required to carry out data analytics as well as machine learning computations. Hence, the cloud layer is where the most crucial and exhaustive data processing tasks take place via the cloud systems. Additionally, the user in this layer has the capability to comprehensively examine and manage the data in a secure cloud setting. While the duration for obtaining insights is extended, it is possible to conduct thorough and complete analysis of the data at this particular stage.

   Finally, it can be seen in Fig. 1 that edge computing is depicted to capture the three top layers, excluding the perception or device layer. This is because according to the framework, all the top three layers are designed to simultaneously exchange information in the IT realm, while the perception layer only includes all devices capable of data collection in the OT realm. The collected data is then transmitted to the IT realm via the edge nodes as depicted in Fig. 3.

3.2 IIoT in smart manufacturing

Smart manufacturing, also known as smart factories, is a concept derived from the IIoT. It envisions a production environment where all systems are completely automated and intelligent. This allows for the management of machinery, facilities, and logistics throughout the manufacturing plant without the need for human interaction. In addition, smart factories provide the setting where these activities occur via the transmission of data amongst various tools and components inside the manufacturing technology network. Hence, this enhances automation and machine learning, enabling more optimal operations and greater cost efficiency compared to relying purely on human control for manufacturing processes. Figure 2 depicts the numerous technologies featured in the implementation of IIoT in smart manufacturing. These technologies include smart logistics, automation, smart mobility, machine learning, cybersecurity, and big data. Each of these technologies provides distinct benefit to the overall functioning of the manufacturing industry.

Smart factories use big data to implement the digitalization of the production process. This results in improved efficiency, delivery, as well as low labor and energy expenses. Machine learning algorithms analyze data generated from sensors and other monitoring devices with the purpose of making instantaneous decisions. This will enhance overall production efficiency while promoting the adoption of IIoT in intelligent factories. Smart logistics, smart mobility, and automation all adopt the use of cobots, actuators, meters, sensors, and other devices to facilitate production, mobility, and logistics within the entire manufacturing ecosystem. And cybersecurity finally ensures the data, tools, and devices, as well as the communication channels between all technologies and the network connectivity in the entire ecosystem, are secured from cyber threats and unauthorized access.

The primary objective of implementing IIoT in factories is to facilitate the integration of interconnected devices and sensors at the network edge, thereby improving real-time machine and human efficiency between all technologies. Additionally, it enables the use of data for more profound analytics and insights, followed by its storage in the cloud. This also facilitates streamlined quality control, optimized machinery management, and improved maintenance, safety, and efficiency. The essential elements of intelligent manufacturing systems include [47].

1. *Physical machines*: These machines perform the practical tasks of moving products through streamlined logistics within the factory. These include loaders, drills, and industrial robots.
2. *Physical tools and devices*: Other physical devices, such as actuators, meters, etc., also control minor movements and monitoring at the low-level stages of each system component within the factory. IT related physical devices within the factory also include routers, edge nodes, servers, computing devices, etc.
3. *Human–machine interface (HMI)*: The HMI mainly oversees and regulates the progression of processes throughout the ecosystem.
4. *Programmable logic controllers (PLC)*: The PLC acts as the intermediary that enables interactive communication between the physical machines and devices, as well as HMI and the other parts of the network.

The above systems mainly work in tandem with other components of the IIoT, such as the cloud, AI, and machine learning, to achieve the required objectives. The integration of cloud, AI, machine learning, and robotic process automation in the IIoT would undoubtedly improve financial performance, operational efficiency, production capacity, product quality, and workplace safety across the entire factory.

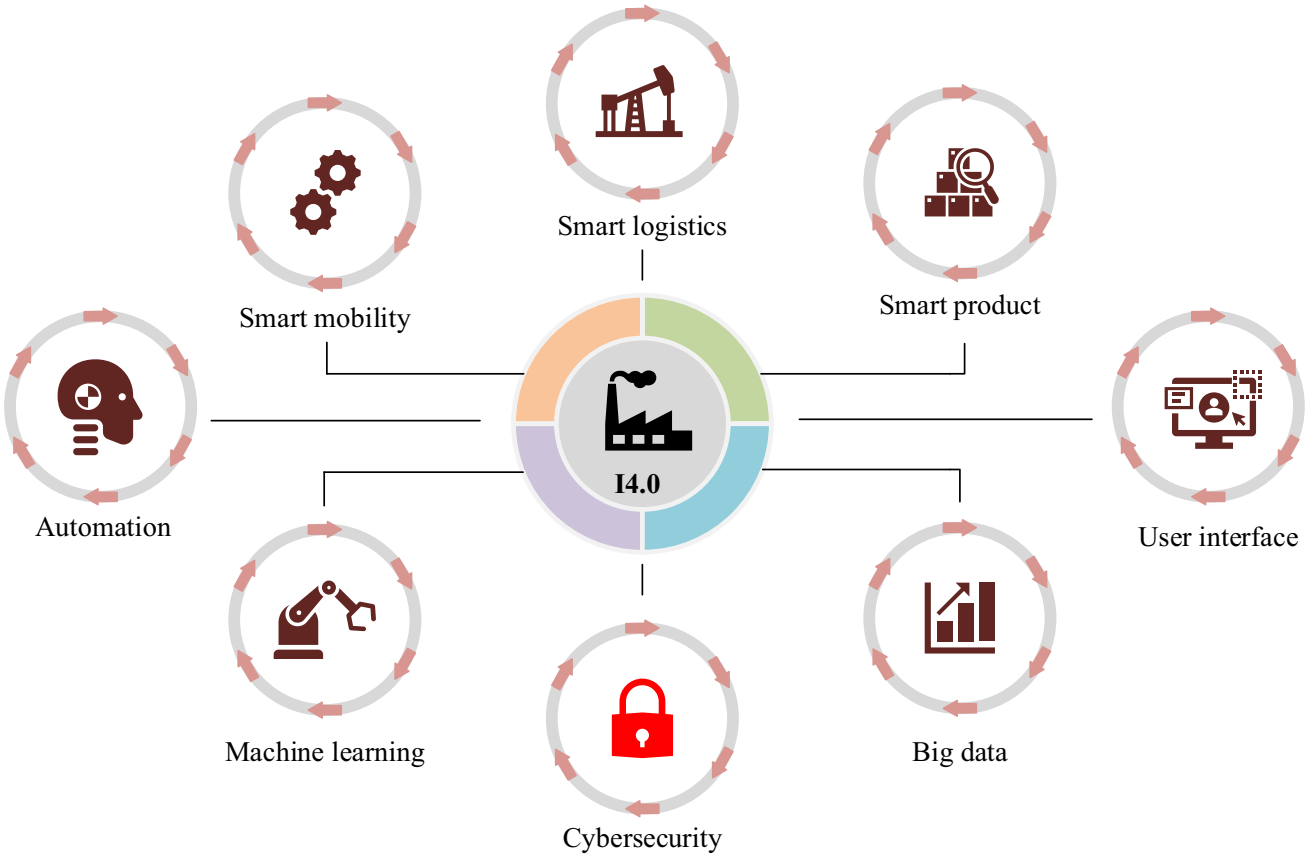

Fig. 2 IIoT in smart manufacturing

4 Attacks and defense mechanisms in the IIoT

4.1 Vulnerable attacks in the IIoT tools and infrastructure

Despite the enormous advantages provided by the IIoT in smart manufacturing, the security and privacy challenges that come with such advantages are diverse. Before delving into the protection mechanisms that would be used to ensure the security of the IIoT, it is important to briefly highlight some attacks that the IIoT can be susceptible to. This will give an insight to the network engineers, systems administrators, as well as users on what to look out for and how to identify and differentiate between various attacks. In essence, this section should serve as an awareness raiser to the IIoT systems administrators on the various IIoT related attacks to keep an eye on. For a more in-depth description and analysis of these attacks, readers can refer to the works in [2, 26], and [17]. While not all the attacks mentioned in those works specifically target the IIoT, the most common ones in smart manufacturing include DDoS, phishing, malware injection/ransomware, spoofing, man-in-the-middle, data sniffing and manipulation, as well as attacks targeting legacy systems. A brief description of these attacks is given as follows.

1. *DDoS*: Distributed Denial of Service (DDoS) attacks impede the flow of services to authorized users. The attacker engages in malicious operations that weaken the computational capacity of systems, rendering them inaccessible or overburdened by inundating the machines with a substantial influx of queries [2]. This attack can be used to target different parts of the IIoT tools and applications, such as routers, network devices, servers, etc.
2. *Man-in-the-middle attacks*: In this attack, the adversary attempts to interfere with or compromise the transmission of information between authorized entities, such as users, tools, and systems. In addition, the adversary may seek to modify the data prior to its dissemination to other entities. This attack can mainly target the communication channels between the IIoT tools and applications through eavesdropping on messages, sniffing and spoofing of network channels, hijacking a session, etc., thereby taking control of tools within the architecture.
3. *Malware injection*: In malware injection, or ransomware, the attacker deploys malware in an attempt to duplicate and transmit harmful code throughout the network, which

might be appended to a trojan application to facilitate effortless infiltration into the system or architecture [2]. The primary objective of these attacks is to inject encryption techniques to encrypt the data or files of a targeted person or organization, with the intention of demanding a ransom in exchange for the decryption key. This attack is very detrimental as it can compromise the entire IIoT data, communication channels, as well as I/O devices.

4. *Phishing*: In phishing, the adversary assumes the identity of a legitimate user and deceives other authorized individuals within the organization into providing their private details on a bogus webpage or persuades them into downloading and installing harmful attachments such as viruses and malware, thus leading to the subsequent disclosure of sensitive data. This attack mainly targets sensitive information, such as login passwords, biometric identity, usernames, and secret credentials. A highly mutant variant of this attack is the spear phishing, where the attackers use specific social engineering content to target a specific organization.
5. *Spoofing*: A spoofing attack involves an individual imitating the identity of a genuine user in order to deceive others and gain unauthorized access to a system, hence enabling the delivery of a malicious payload. By using methods such as IP spoofing, the adversary is able to manipulate the source IP address associated with the sent packets to deliver an exploit. A variant of such attack is also available in biometric systems, where the attacker uses a fake biometric template to fool the system in order to gain access.
6. *Data sniffing and manipulation*: Sniffing and manipulation are all attack variants that can expose the confidentiality and integrity of the IOP systems. Such attacks make it easier to sniff or manipulate data in the transmission channels through eavesdropping and replay. It is often easier to perform these attacks on unencrypted data or communication channels that aren't secure.

4.2 IT and OT convergence security threats

The convergence of information technology (IT) with operational technology (OT) is the basis of the IIoT. Physical components such as robots, actuators, meters, monitors, and edge nodes represent the OT, while IT encompasses both onsite IT infrastructure and cloud-based IT services, which are used for storage and analytics purposes. The edge nodes provide communication between OT and IT systems by using the edge network. However, security is often considered within the realm of IT as a client–server paradigm, whereby the exchange of information between the client and the server takes place using established protocols like IP, UPP, TCP, and HTTP [2]. Figure 3 depicts the IIoT ecosystem in smart manufacturing with emphasis on IT/OT convergence.

IT and OT in a smart manufacturing setting offer several advantages, including improved efficiency and seamless communication, as well as access to real-time data. Nevertheless, they are very vulnerable to various cyber threats. An accomplished cyber-attack on IT systems can lead to the loss of sensitive data that might forever be irreplaceable. Other consequences are the huge financial loss and system downtime. On the contrary, OT is specifically geared to facilitate secure and dependable industrial processes. Unfortunately, the OT systems and components were not originally developed with security as a priority. In order to ensure security, OT components are either kept apart from susceptible areas or protected by physical security and safety precautionary measures [48]. The security measures used for OT systems are unreliable and may potentially reveal weaknesses that may be taken advantage of by malicious actors. OT systems may be better protected against attacks from other networks if they use network segmentation, but they may not be safe enough against internal threats. However, malicious software may be readily installed on the network to launch attacks on these systems. Hence, comprehending every potential attack vector on every level of the IIoT infrastructure is crucial to developing a comprehensive threat mitigation strategy [49].

Generally, the IIoT systems are considered some of the most vulnerable systems targeted by cyberattacks in both the IT and OT realms; as such, the security of IT and OT play a crucial role in protecting the critical heterogeneously interconnected manufacturing systems against such attacks. Figure 4 depicts the general taxonomy of IIoT attacks based on attack vector, attack target, attack impact, and attack consequences in both physical (OT) and cyber (IT) scenarios [2].

A comprehensive grasp of this attack taxonomy will help facilitate the secure and robust implementation of defenses within the entire IIoT, thereby proactively recognizing and mitigating threats while safeguarding essential tools and critical infrastructure from unauthorized breaches.

Other potential vulnerabilities that manifest due to IT and OT convergence include the following:

1. *Vulnerabilities in communication protocols*: The communication protocols that aid with the IT and OT convergence via the edge nodes can be considered the vital aspect of enabling such convergence functionality. However, some of the well-known transmission interfaces such as Modbus and Profibus have been proven vulnerable [50]. As a result, the use of such insecure transmission interfaces can lead to susceptibility against numerous attacks targeting the communication protocols.

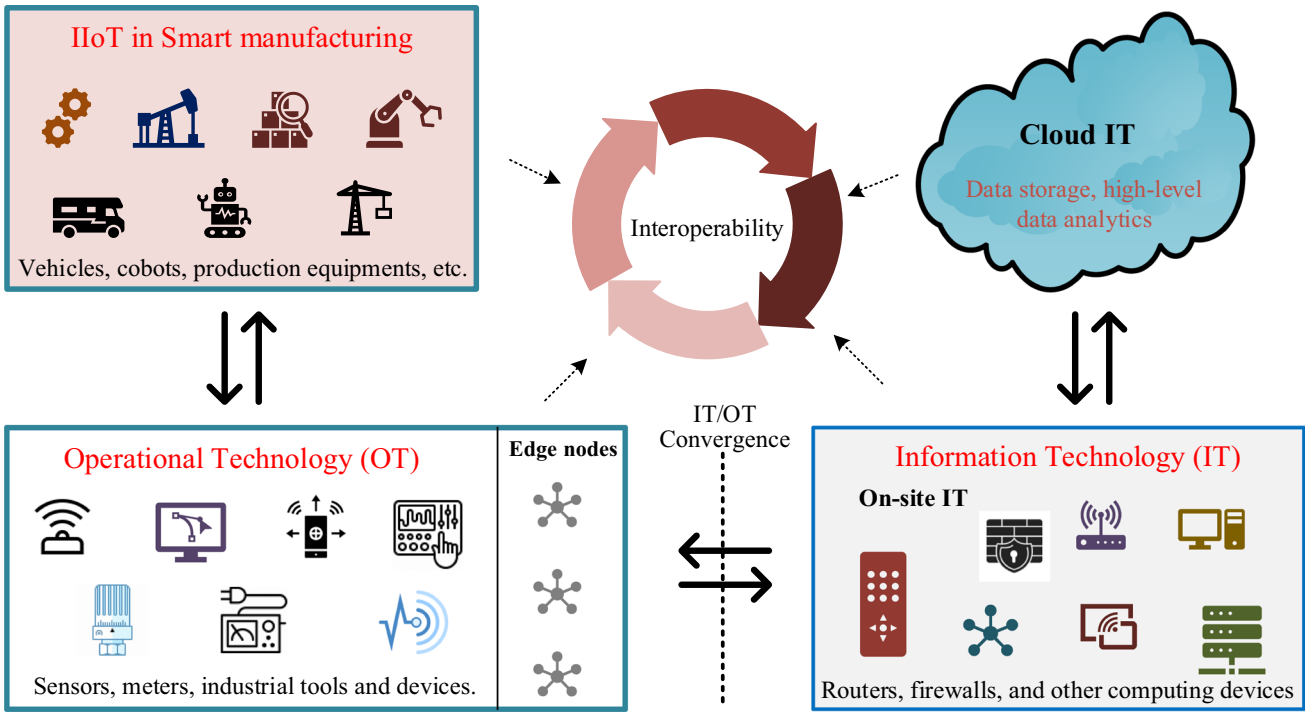

Fig. 3 The IIoT ecosystem in smart manufacturing with emphasis on IT/OT convergence

2. *Inadequate authentication mechanism*: Weak authentication and authorization mechanisms also exist within those communication channels. As an instance, both NB-IoT and Wireless-HART lacks functionality and support for secure authentication in IIoT environments [51]. Likewise, Modbus and MQTT are susceptible to flaws that could compromise the authentication and integrity required to secure the transmission channels.
3. *Inadequate data security*: Given that most of the adopted tools for secure transmission interfaces are vulnerable to attacks, the security of the data transmission between different clients and access points cannot be guaranteed. Therefore, without the guaranteed security of the transmission channels, the data itself is insecure.
4. *IIoT application vulnerabilities*: Most IIoT smart manufacturing industries lacks security architecture in their design. Additionally, inadequate security measures implemented in the design by external providers in the IIoT can facilitate the infiltration of harmful viruses, malwares, trojans, and botnets into the operational environment. This can lead to compromising the SCADA and other systems.
5. *Lack of security awareness*: There is a lack of security awareness and knowledge to the security measures and regulations in industrial control systems setting. Furthermore, this is exacerbated by the lack of standard technologies, secure remote controls systems, and publicly available technical knowledge.
6. *Weak delineation between IT and OT*: Considering the segregation between the IT and OT technologies is only achieved via the edge nodes, the security of such nodes must be strengthened. Moreover, other enhanced security mechanisms can be incorporated in the nodes.
7. *Lack of collaboration*: The collaboration between IT and OT teams has been uncommon, resulting in potential security oversights that may amplify intricacies, escalate operational expenses, and expose vulnerabilities that malicious actors can use. In order to guarantee IIoT security, it is essential for separate teams to give priority to working together and exchanging information in a seamless manner.
8. *Inadequate insight*: IT often depends on asset identification and configuration to get a comprehensive and accurate understanding of the managed environment. OT systems need to possess the capability to coexist in this context and provide functionalities that operate with ease via remote setup and administration. If an administrator lacks access to an OT device, they are unable to effectively ensure the security and management of that device, which subsequently has the potential to result in security risks.
9. *Vulnerabilities in SCADA implementation*: SCADA control systems and PLCs are regarded as the central components of every industrial control system in smart manufacturing [52]. However, some SCADA systems

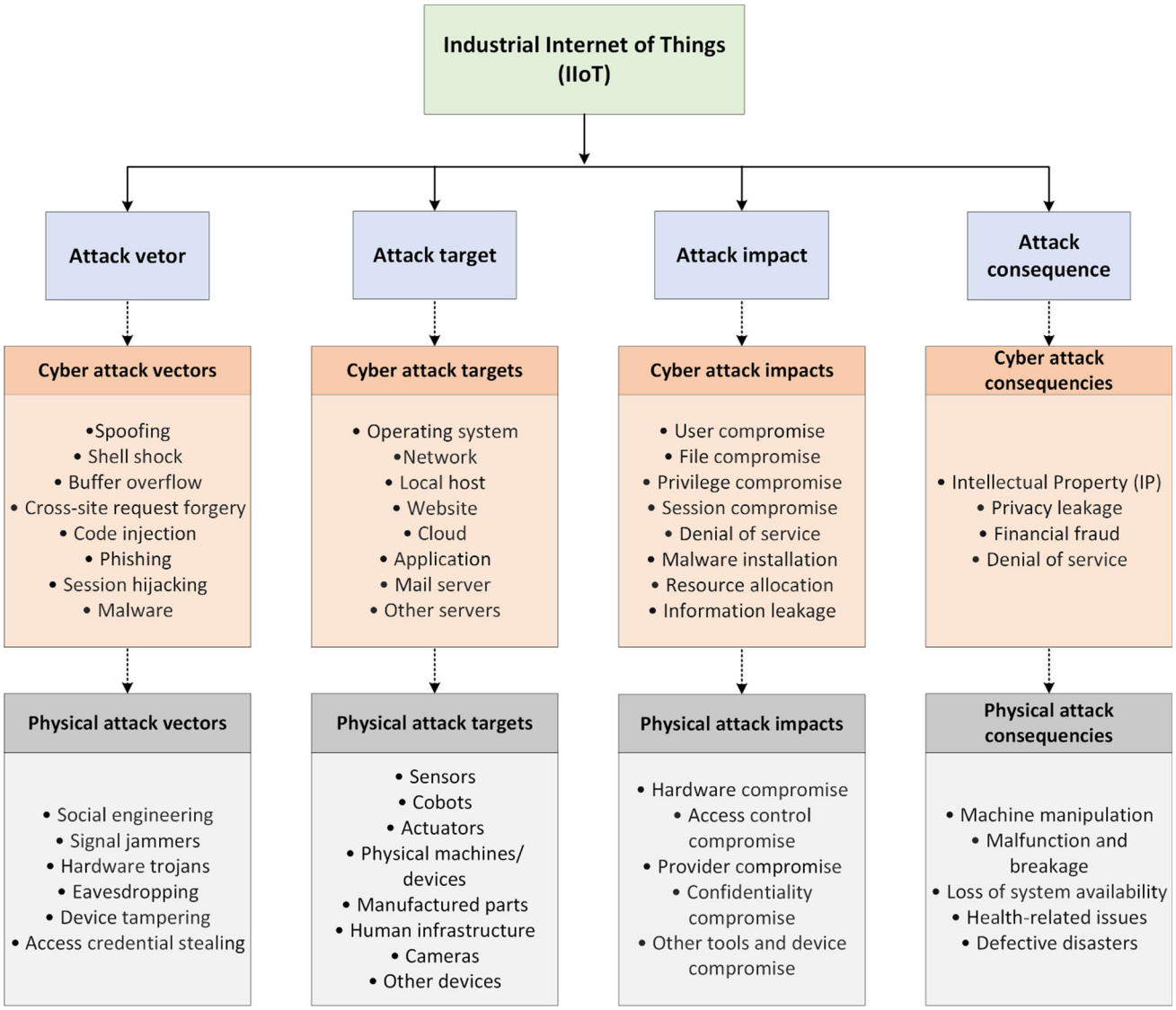

Fig. 4 Attack taxonomy of the IIoT [17]

continue to use unsupported operating systems like Windows XP, while many IIoT systems depend on obsolete firmware or vulnerable third-party components [52]. Nonetheless, ensuring security for both the SCADA systems and PLCs is of utmost importance due to the many vulnerabilities they present in both the firmware and software components of the IIoT systems, which include a range of cyber threats such as ransomware, spoofing, DoS/DDoS, worm-based malware, etc. Major weaknesses of such systems include the following:

a. Inadequate understanding of the devices associated with SCADA and PLCs systems from both the OT and IT sides.
b. Lack of secure authentication mechanisms for access control and data protection.
c. Lack of security measures related to remote access.
d. Software design without adequate security consideration.
e. Enabling unlimited uploads on such systems and deploying PLCs operating system with vulnerabilities.

Likewise, considering that the majority of smart manufacturing facilities include several devices intended for remote access, other attack vectors exploit vulnerabilities such as:

1. Intercepting unencrypted passwords on ICS networks.
2. Utilizing preconfigured passwords or SSH keys for firmware authentication.
3. Exploiting the code execution process of a device in order to get unauthorized access to confidential data.

4. Establishing a connection with a device with a serial interface.
5. Lack of account suspension or deactivation regulations in place.

4.3 Recent defense mechanisms for IIoT tools and infrastructure in smart factory

In an age of rapid digital expansion, the need of securing IIoT platforms and technologies is paramount. The IIoT smart manufacturing tools and applications need to be built on rigid and secure defense mechanisms. Therefore, this section delves into the novel security and privacy-preserving techniques devised to defend the IIoT's infrastructure, digital modules and services, various tools and devices, data, users, and the network that interconnects these elements from various cyberthreats.

Considering the vast landscape of the IIoT ecosystem that needs protection, a meticulous approach must be taken to ensure that no facet is left unguarded. Whether it's controlling access to physical and virtual resources, real-time monitoring for anomaly detection, or ensuring that data is handled with the utmost integrity and care, each dimension has its significance. Also, the defense mechanisms ensure both IT and OT security are taken into consideration. These mechanisms include authentication, access controls, network security, data security, real-time monitoring and incidence response, cloud security, data privacy, and other countermeasures.

4.3.1 Authentication

In the IIoT infrastructure, a robust authentication system is paramount to ensure that access is granted only to authorized entities. Various authentication mechanisms have been proposed for IIoT in smart manufacturing, however, a large number of these proposals still remain vulnerable to attacks such as phishing, spoofing, impersonation, privilege insider, etc. To address these problems, Hammad et al. [53] propose a novel method of mutual authentication among the modular manufacturing system unit, users, and the server through the facilitation of secure communication within the IIoT ecosystem. This is specifically applied in the context of smart manufacturing. The approach achieves secure authentication by issuing session keys. The strategy also exhibits strong resilience against a wide range of security threats while surpassing the performance of other existing schemes. Tanveer et al. [54] introduce CMAF-IIoT, an authentication framework for IIoT that combines chaotic maps with the resource-efficient AE scheme ASCON [55] in order to tackle the aforementioned security challenges. CMAF-IIoT facilitates dependable connectivity between smart manufacturing devices (SMDs) and consumers. The framework begins with users' local authentication on their smart devices, and after both parties have successfully authenticated one another via the gateway, the formation of a session key with the SMD follows. Users can then safely get real-time information from SMDs installed in the IIoT ecosystem by using the session key. The security of CMAF-IIoT is verified using both formal and informal security evaluations. In [56], Want et al. present an efficient authentication mechanism, known as AP-CDE, for facilitating the interchange of data across different domains in the IIoT. This protocol utilizes anti-collision hash functions, bitwise exclusive-OR operations, and Chebyshev polynomial operations. AP-CDE security is attained by the use of robust (formal) and nonmathematical (informal) analytical techniques. The analytical findings demonstrate that the designed procedure is capable of withstanding a range of well-established threat vectors. Moreover, a comprehensive analysis is conducted between AP-CDE and other relevant protocols to confirm that it is better in terms of security, functionality, communication overheads, and computational efficiency.

Srinivas et al. [57] present a novel, secure-proof user authentication key agreement approach that restricts access to selected IoT sensing devices in the IIoT ecosystem to authorized users only. The system utilizes the fuzzy extractor for biometric verification. Furthermore, the proposed solution uses a three-factor authentication approach based on smart cards, passwords, and personal biometrics to enhance security. It also makes it easier to change passwords or biometrics with an aided biometric template protection method, so smart cards can be taken away if they are lost, stolen, or hacked. Furthermore, the suggested system is characterized by its lightweight nature. Several security analyses conducted on the system prove its robustness against various attacks while achieving an efficient computational cost. Another multifactor-based authentication scheme for the IIoT in smart manufacturing utilizes pre-established key agreements between smart devices and gateway nodes while using biometrics [58] to enhance verification between users. The scheme provides robust security against different attacks. In [59], Patel et al. propose an inter-device authentication technique using Elliptic Curve Cryptography (ECC), which offers superior security and efficiency compared to other comparable schemes in the same setting. In addition, the authors conducted a thorough formal security study utilizing the random oracle-based ROR framework and an informal security analysis over the Dolev–Yao channel. The technique is secure and efficient. Xu et al. [60] introduced a reliable cross-layer authentication scheme that relies on quantum walk-on circles. The system utilizes random hash coding on multidomain physical-layer resources to securely encode and

decode device identifiers. It employs a privacy-preserving protocol based on quantum walk to maintain a high level of code privacy, which is determined by the number of physical resources used. An upper limit for decoding errors is determined, and a nonconvex integer programming problem is developed to minimize this limit and estimate the security performance. The space of one-time keys for encryption is generated to demonstrate the maintenance of high privacy and scalability advantages over conventional and quantum computers. Their approach provides an exceptionally high degree of security and privacy while maintaining minimal latency, even in the face of a threat. Cui et al. [61] present an anonymous authentication mechanism with consideration for semi-trusted entities in IIoT.

Recently, researchers are beginning to focus on designing devices with inbuilt authentication mechanisms in the OT context to mitigate attacks emanating from the edge nodes. Such techniques include the works of El-Zawawy et al. [62] and Koprov et al. [63]. In [62], the authors provide an innovative protocol called HASAO (Honey-list Authentication for SIIoT with Autonomous Objects) for the purpose of key agreement and authentication. HASAO facilitates streamlined and safeguarded end-to-end communication across devices within the same or separate swarms. It also addresses the issue of incorporating a practical system model that can accommodate several sorts of dynamic objects concurrently. As a result, the authors apply honey lists, which are equipped with algorithms designed to prevent password guessing. In addition, they deploy mutual authentication methods to ensure the security of HASAO against various attacks, especially in situations involving communication over public channels. In [63], the authors suggest using Physical Unclonable Functions (PUFs) to identify and authenticate industrial equipment, such as cobots, actuators, SCADA systems, etc., over a network. In order to identify machine assets within a network, the authors decided to use the vibration that machines and their integrated mobile components release, given that the moving parts of machines are considered to produce unique patterns of vibration.

The widespread adoption of blockchain for IIoT has led to its utilization in many recent authentication techniques. Zhang et al. [64] introduced a blockchain-based multifactor device authentication protocol for cross-domain in IIoT. Shen et al. [65] proposed a similar cross-domain mechanism based on identity-based signatures. In [66], Li et al. employ blockchain technology to authenticate IIoT devices using PUFs. The authors subsequently used the CRPs for model training to safeguard the PUFs. To ensure secure transmission protocols and user security while optimizing blockchain node selection for the IIoT, Sharma et al. [67] developed an approximate fully homomorphic encryption neural network built on block-chain technology.

4.3.2 Access control

In the modern digital landscape, ensuring secure, selective access to critical infrastructure is paramount. Uncontrolled or poorly regulated access can compromise the stability, security, and performance of a system, leading not just to operational hitches but also potential data breaches. With the IIoT ecosystem playing such a pivotal role in processing and safeguarding vast quantities of data, the adoption of a well-structured, role-based access control becomes paramount.

Aside from the common open-source access control mechanisms like role-based [68], rules-based [69], attributes-based [70], etc., researchers are now focusing on designing access control mechanisms specific to the domain use cases in terms of the level of permission to be granted and to which party that specific permission should be granted. In [71], Saha et al. introduce DHACS, a Decentralized Hybrid Access Control System for Smart Contracts, which is specifically tailored for IIoTs in smart manufacturing. The objective of DHACS is to enhance the current access control mechanism in IIoTs by ensuring transparency, dependability, and robustness through the integration of three different access control mechanisms: role-based, rule-based, and organizational-based. The architecture utilizes blockchain capabilities to provide an integrated hybrid access control system via the supply of smart contracts. The technique outperforms other access control-based methods in terms of security, computational expenses, storage complexity, and energy usage. Cui et al. [72] present multi-authority access control with a revocation mechanism.

Other access control mechanisms built on blockchain technology include the works of Wang et al. [73], where the authors provide a smart contract token to enable decentralized control in IIoT. The technique uses three distinct smart contracts: Token Issue Contract (TIC), User Register Contract (URC), and Manage Contract (MC) to oversee and administer diverse events in IIoT. In addition, Nth-degree Truncated Polynomial Ring Units (NTRU) encryption is used to ensure security against quantum attacks. Bera et al. [74] proposed a blockchain-based access control for the IoD (Internet of Drones) within the IIoT ecosystem that allows secure communication. Nakamura et al. [75] exploit smart contract capabilities for access control, while Liu et al. [76] leverage the Hyperledger fabric capability. Moreover, techniques proposed by Ding et al. [77] and Nasiraee et al. [78] achieved secure attribute-based access control using blockchain technology. Figueroa-Lorenzo and his team [79] employed a permissioned Hyperledger fabric blockchain method to guarantee dependable control access in the IIoT infrastructure.

4.3.3 Data security

In the realm of IIoT, data stands as the bedrock upon which platforms and services function. Therefore, ensuring the utmost security of this data is not just a necessity but a duty, considering the significant value and sensitivity it holds for users and organizations alike. From access controls that employ sophisticated authentication mechanisms to backup strategies that ensure swift recovery in adversity, each facet of data handling must be approached with meticulous care. As such, every IIoT ecosystem must recognize the multilayered challenges of data security and respond accordingly by instituting a comprehensive system to address them. With this aim, researchers have proposed different data security mechanisms. Salim et al. [80] introduced an Information Fusion-based Federated Learning Framework (FL-CTIF) for securing IIoT ecosystems. An all-encompassing cyberattack dataset is constructed using information fusion, wherein updated feature selection is implemented to enhance the precision of cyber-attack detection. Afterward, an ANN model based on federated learning is integrated to decrease the number of training periods, taking into account the user's level of contentment and the absence of improvement in the average accuracy of each attack vector. Halder et al. [81] introduced a data storage and sharing solution that enables scalable analytics on encrypted time-series data known as SmartCrypt. The technique ensures end-to-end encryption using a novel symmetric homomorphic encryption method that allows users to protect and selectively share their encrypted data in private even when unauthorized users are present.

Recently, Gilles et al. [82] proposed a strategy that utilizes open-source software to enhance data sharing and authentication of devices located outside of the premises. The primary goal is to ensure the secrecy and integrity of data exchanges with the rest of the IIoT devices based on end-to-end encryption. The technique also uses a trusted platform module as a secure component to safeguard the confidential information stored inside devices. To mitigate the challenges of the real-time training requirement in IIoT, the lack of defense mechanisms against insider threat vectors, and the performance-privacy tradeoff in fusion data, Lin et al. [83] present a novel approach using transfer learning-based secure data fusion (TSDF) for IIoT. The technique is made up of three parts: a guidance-based deep deterministic policy gradient (GDDPG) algorithm for task categorization, a transfer learning-based GDDPG for grouping task receivers, and a multi-blockchain method for preserving anonymity.

Other blockchain-based data security approaches include the recent use of the multi-blockchain approach by Umran et al. [84]. The authors have chosen to use the incremental aggregator subsector commitment, rather than the Merkle tree and multi-chain proof, to facilitate fast data sharing and authentication. Lu et al. [85] proposed a group signature scheme based on smart contracts and proxy re-encryption for cloud storage solutions in IIoT to ensure efficient data sharing and storage. Security proofs and performance evaluations validate the efficiency of the technique. Jiang et al. [86] introduced a strategy for decentralized data sharing in IIoT using edge computing and blockchain. The PoST consensus method is suggested as a solution to fulfill the data storage and transmission needs of data owners in IIoT data-sharing networks. In another approach, the authors [87] use data packet transactions (DPTs) and data analytics service transactions (DASTs) smart contracts to ensure a secure and feasible data sharing IIoT platform. In [88], Yu et al. introduced a unified identity authentication system that supports both traceability and revocability. This system not only mitigates data sharing and storage challenges, but also manages access control, updates and deletes information in smart factory data, and monitors and revokes access for unauthorized and illicit individuals. Kumar et al. [89] proposed a blockchain-based decentralized IIoT to overcome the data dissemination challenges in IIoT. The suggested paradigm utilizes a secure peer-to-peer (P2P) network in which every node communicates with another. Yu et al. [90] present a consortium blockchain-based cross-domain data sharing mechanism in IIoT via group signature. Meanwhile, Ma et al. [91] introduce blockchain-enabled dynamic and traceable data sharing scheme in smart factories via authentication, a tracking algorithm, and an online-offline encryption and outsourced decryption mechanism. In another secure data sharing technique. Xu et al. [92] incorporate into the sharing platform a fine-grained access control mechanism that relies on hierarchical attribute-based encryption and multi-level authorization. This mitigates data privacy leakage while ensuring a secure data exchange. Table 3 provides a summary of IIoT protection mechanisms, including authentication, access control, and data security, along with their respective methodologies and threats that are mitigated. Finally, Abdullahi et al. [93] also discuss the different biometric template protection mechanisms, including cancellable biometrics and biometric cryptosystems, such as the works in [94–96].

4.3.4 Network security

The rapid acceptance and proliferation of IIoT in smart manufacturing has led to an increasing deployment of smart devices within the IIoT infrastructure, resulting in heterogeneous interconnectivity and heightened cyber threats. Consequently, effective strategies for monitoring and safeguarding the IIoT network are essential for maintaining the integrity, confidentiality, and availability of data across the infrastructure. Most network security mechanisms are built on the premise of segmentation, real-time monitoring and incident response, as well as network configuration and audit to manage network performance while ensuring its security

Table 3 Summary of the IIoT protection mechanisms, including authentication, access control, and data security, with their specific methodologies and mitigated threats

Protection mechanisms	References	Specific methodologies used	Mitigated threats
Authentication	[53–67]	Mutual authentication between modular manufacturing systems	Privilege insider phishing impersonation
		Chaotic maps and resource efficient AE	Man-in-the-middle
		Lightweight cryptography (LWC)-based authenticated encryption, associative data (AEAD) primitive AEGIS, and hash function	User anonymity
		Anticollision hash functions, bitwise exclusive-or operations, and Chebyshev polynomial operations	DoS
		Fuzzy extractor, three-factor authentication, and biometric template protection	Identity guess replay
		Pre-established key agreement and biometrics	Mutual authentication
		Inter-device authentication technique using Elliptic Curve Cryptography (ECC)	IoT sensing device capture attacks
		Secure cross-layer authentication framework based on quantum walk on circles	Credential stuffing
		Random hash coding on multidomain physical-layer resources	Brute-force
		Honey-list based authentication	
		Physical unclonable functions (PUFs) via unique vibration pattern (fingerprinting)	
		Anonymous authentication mechanism for semi trusted entities in IIoT	
		Blockchain-based authentication schemes	
Access control	[71, 72, 74–79]	Decentralized hybrid access control system	Quantum attacks
		Smart contracts and Nth degree truncated polynomial ring units encryption (NTRU)	User anonymity
		Multi-authority access control with revocation	Key loggers
		Other blockchain-based access control mechanisms	Spoofing,
			Eves dropping
			Brute force
			Credentials stiffing
Data security	[80–92]	Fusion-based federated learning framework	Data manipulation ARP poisoning MITM SSL-based
		End-to-end encryption using symmetric homomorphic encryption	Leak prevention
		End-to-end encryption for secure out-premise devices	DNS flood-based DDoS
		Transfer learning-based secure data fusion (TSDF)	Insider threats
		Incremental aggregator subsector commitment	Data sniffing Malware injection
		Group signature scheme based on smart contract and proxy re-encryption	Ransomware
		Edge-computing and blockchain under multiple-leader and multiple-follower Stackelberg game concept	

Table 3 (continued)

Protection mechanisms	References	Specific methodologies used	Mitigated threats
		Data packet transactions and data analytics service transactions smart contracts	
		Enhanced secure data sharing and storage via unified identity authentication	
		Blockchain-based decentralized IIoT via secure peer-to-peer network	
		Other blockchain-based data protection mechanisms	

against cyber threats. In addition to conventional security measures such as firewalls, classic intrusion-detection systems, and antivirus softwares, researchers have recently been proposing novel approaches for securing networks in the IIoT infrastructure. These techniques include the following:

Oliveira et al. [97] proposed using machine learning to plan the deployment of secure virtual network functions (VNFs) based on the performance of network function virtualization (NFV) in order to protect IIoT systems from DDoS attacks. The suggested model leverages a robust peer-to-peer (P2P) network, whereby every node engages in interactions with other nodes. In [98], Siriweera et al. introduced an architectural modeling process for software reference architecture for crosschain-based smart manufacturing. The technique meets the critical quality of service (QoS) requirements for guaranteeing network security and privacy while also preserving scalability and interoperability. Atutxa et al. [99] introduce a system that validates certificates inside a network, relieving restricted IIoT devices of this duty and instead using a network element with more resources. This strategy improves security by ensuring that a thorough verification of the server certificate is consistently carried out. Furthermore, it enhances performance by transferring resource-intensive activities from IIoT devices to a network node with greater resources. Khan et al. [100] introduce a deep-autoencoder-based intrusion detection system that can accurately differentiate between malicious activities and normal operations in IIoT-driven industrial control systems networks (IICS) in real-time. The model utilizes an LSTM auto-encoder architecture to accurately detect intrusive events inside the IICS networks. Deshpande et al. [101] present an architecture that incorporates cloud-based data transmission using augmented reality (AR) for visualization, interpretation, and data analytics. The AR system utilizes a Bayesian network to allow users to enter desired quality metrics and get real-time process suggestions.

Recently, Illy et al. [102] proposed a low-latency and robust deep learning-based collaborative intrusion detection and prevention system that is secure and efficient in both resiliency and response time. The architecture employs a lightweight deep neural network to carry out classification, which guarantees identification of intrusions and a multi-class categorization of detected anomalies. Chaudary et al. [103] designed a software-defined network-enabled multi-attribute for secure communication in IIoT. The author utilized a cuckoo-filter-based fast-forwarding scheme, attribute-based encryption, and peer entity authentication to ensure secure communication within the IIoT ecosystem. Pokhrel et al. [104] proposed a multipath transmission control protocol for efficient IT/OT convergence while overcoming most challenges associated with such convergence. Zhu et al. [105] proposed a smart collaborative routing protocol based on a one-hop delay model and sub-protocol generation. The strategy cuts down on end-to-end delay while improving transmission speed and security. Jagtap et al. [106] proposed a stacked deep learning model for industrial control systems against cyber threats. Wu et al. [12] present an intelligent network slicing architecture for IIoT, offering a comprehensive investigation and analysis of network slicing management. Moreover, Yazdinejad et al. [107] utilize federated learning to construct a threat hunting system named "Block Hunter" that autonomously detects threats in blockchain-based IIoT networks. It employs a cluster-based framework for identifying unusual patterns, together with machine learning models, inside the federated setting. Other techniques that ensure cloud security in the IIoT include those described in [108–112].

4.3.5 Data privacy

The massive interconnectivity of IIoT brings forth not just security challenges but also privacy challenges. Moreover, contrary to the use of protection mechanisms and policies to ensure the security of data, data privacy aims at ensuring the proper collection, retention, usage, deletion, and storage of data. Data privacy mostly focuses on the rights of users with respect to their personal information. However, data privacy and data security are closely related, as only

data that passes through both processes is deemed protected and usable. Some of the techniques covered in the previous protection mechanisms also ensure data privacy simultaneously. Nonetheless, some studies have specifically focused on ensuring data privacy. These include the work of Humayun et al. [113]. The authors provide a comprehensive framework for energy resource optimization through privacy improvement. It ensures the three levels of privacy, including data, identity, and location, are maintained. Xu et al. [114] present a trust computing and hierarchical trustful resource assignment algorithm, which utilizes the Vickrey–Clarke–Groves mechanism to distribute the necessary resources for wireless communication between IIoT devices and gateways. It also focuses on the allocation of CPU resources for handling data at the CPC. This guarantees privacy, safety, and trust estimation. Chen et al. [115] made improvements to the privacy of DeepPAR, an asynchronous deep learning mechanism that preserves privacy.

Recently, various privacy-preserving federated learning techniques have been developed to preserve users' data privacy. One of these methods is described by Han et al. [116], who create a sampling-based intermittent communication strategy and budget allocation mechanism to improve accuracy while protecting privacy and facilitating communication in the IIoT. Bugshan et al. [117] present a service-oriented architecture that utilizes edge and cloud computing to support residual network-based federated learning with differential privacy. The framework identifies the important components and outlines a service model for building locally trained models that can be trusted. A privacy-preserving local model aggregation mechanism that guarantees reliable execution while maintaining privacy is realized. Li et al. [118] designed an alternating optimization strategy algorithm based on a flexible and robust aggregation rule known as the auto-weighted geometric median. The technique ensures privacy and security while sustaining high performance. In their work, Wang et al. [119] develop a routing protocol that protects data privacy by enhancing the community identification method info-map and dividing the routing area into optimal subdomains. This partitioning serves as the basis for implementing the deep reinforcement learning algorithm, which is used to construct a gateway deployment model. Federated reinforcement learning is then used for a universal gateway deployment model, making sure that the routing data is kept private while eliminating areal differences.

In another approach, Wang et al. [120] proposed a universal detection strategy where each local model is trained using a deep reinforcement learning algorithm. The technique improves anomaly detection accuracy while ensuring data privacy within IIoT devices. Zheng et al. [121] proposed an unsupervised recurrent federated learning algorithm to ensure data privacy in mobile-edge computing networks within the IIoT.

Other blockchain-based privacy-preserving schemes include the work of Pandey et al. [122]. The authors introduced a secure SVM privacy-preserving training strategy that utilizes blockchain-encoded IoT data derived from IIoT. Data transmitted over the IIoT is encrypted prior to storage on a decentralized system using the Paillier and homomorphic cryptosystem algorithms. The technique not only ensures privacy preservation but also provides profound security. Bao et al. [123] proposed a blockchain-based identity management system for the IIoT that preserves privacy. The technique is capable of fully supporting the ideal privacy properties—namely unforgeability, blindness, unlikability, traceability, revocability, and public verifiability—through the utilization of blockchain technology and a variety of cryptographic tools. Blockchain-enabled privacy-preserving authentication schemes [124, 125] are also being introduced to ensure data privacy and security in the IIoT.

Furthermore, the fusion of blockchain and federated learning for privacy preservation in the IIoT has been recently recognized by the research community. Singh et al. [126] use the federated layer to facilitate network-automated local learning and communication with the global model, which is verified by blockchain miners in the networks. Duy et al. [127], on the other hand, leverage a local training strategy that eliminates the necessity for centralized data collection. The technique also utilizes well-orchestrated software-defined networking, differential privacy, and fully homomorphic encryption to ensure robust security and privacy. Table 4 provides a summary of IIoT protection mechanisms, including network security and data privacy, along with their respective methodologies and threats that are mitigated.

5 Guide to a secure IIoT tools and infrastructure in smart factory

This section provides the guidelines for adopting and deploying secure, open-source, and privacy-preserving AI-based IIoT in smart manufacturing. The guidelines use the best security measures for mitigating cyberattacks, taking into account the digital services, modules, and other IoT devices in the IIoT network. Thus, the guidelines ensure that the defense mechanisms highlighted in Sect. 4 above can be adopted and deployed in accordance with the protocols itemized and explained in this chapter. It is worth nothing that the guidelines adhered to the latest and most stringent requirements defined by the European Commission and other relevant regulatory authorities, as discussed in Chapter 2. Also, another point worth noting is that the guidelines are documented in cognizance with both IT and OT realms in mind. As such, they can be applied to systems, modules, data, devices, networks, etc. that fall within both realms, thus ensuring in-depth coverage of the entire IIoT ecosystem.

Table 4 Summary of the IIoT protection mechanisms, including network security, cloud security, and data privacy, with their specific methodologies and mitigated threats

Protection mechanisms	References	Specific methodologies used	Mitigated threats
Network security, including real-time monitoring and incidence response, segmentation, and cloud security	[12, 97–112]	Machine learning based network function virtualization	DDoS
		Architectural modelling process based on cross chain	Buffer flow
		In-network server certificate validation system	Flame
		Long short-term memory deep auto-encoder architecture	Seismic
		Augmented reality and Bayesian network	Qudu
		Lightweight deep neural network and multi-class categorization	Anomaly detection
		Cuckoo-filter-based fast-forwarding, attribute-based encryption, and peer entity authentication	IP spoofing
		Multipath transmission control protocol	Signal jammers phishing
		Smart collaborative routing protocol based on one-hop delay model and sub-protocols generation	
		Stacked deep learning model	
		Intelligent network slicing architecture	
		Cluster-based and machine learning frameworks	
Data privacy	[113–127]	Energy resource optimization through privacy improvement	Collusion
		Hierarchical trustful resource assignment and trust computing algorithm that utilizes vickrey-clarke-groves mechanism	Poisoning
		Privacy-preserving and asynchronous deep learning mechanism	Data leakage
		Sampling-based intermittent communication strategy and budget allocation mechanism	Anomaly detection
		A privacy-preserving local model aggregation mechanism	
		Alternating optimization strategy-based auto-weighted geometric median	
		Data privacy-aware routing protocol using deep and federated reinforcement learning	
		Universal anomaly detection model with deep re-enforcement learning algorithm	
		Unsupervised recurrent federated learning algorithm	
		SVM privacy-preserving training strategy with blockchain encoded IIoT data	
		Blockchain and diversified cryptographic tools	
		- Network-automated local learning	
		Software defined networking with differential privacy	
		Other blockchain-based privacy-preserving schemes	

5.1 Guide to secure digital services and modules

5.1.1 Authentication

For the vast majority of systems and networks, authentication is the first layer of protection. Prior to accessing the network, tools and applications should be verified with the goal of eliminating malicious devices from the IIoT ecosystem, thus preventing the infiltration and dissemination of falsified data. Authentication mitigates a variety of attacks, including phishing, keyloggers, credential stuffing, brute force, and man-in-the-middle attacks, among others. Guidelines to be considered for the IIoT authentication include.

1. *Modify default system settings*: As a first measure, the default credentials that come with all the IIoT tools and system applications should be modified. System administrators and users should, by all means, avoid running devices with default credentials.
2. *Avoid using the same logins*: Additionally, system administrators and users should avoid reusing the same credentials across multiple devices. If the authentication mechanism is a password, at least three letters should be modified to some arbitrary random word that the user can remember. If it's a hardware token, a new one should be generated, and if it's a biometric, a biometric template protection mechanism should be incorporated into the authentication system such that an old template can be revoked and replaced by a new one in the event of an attack.
3. *Ensure device credentials are not hard-coded*: Following the reset of a password or token, it is essential to disable the functionality of the default login. However, if the system is still functional on such default logins, it is possible that the credentials have been hard-coded. In such a scenario, it is advisable to replace the device or opt for an alternative product.
4. *Adopt a good authentication mechanism*: A soundproof authentication mechanism(s) from the novel techniques discussed in Sect. 4.3.1 should be adopted and deployed. Preferably, two factor authentication such as biometrics and one-time password/hardware token should be given utmost consideration.
5. *Frequent password update*: If by any means system administrators and users decide to use a password/token for access, a frequent password and token update policy should be adopted by the administrators. It can be quarterly or every three months interval.
6. *Ensure default hardware reset devices are protected*: Furthermore, ensure that any hardware reset procedures on all IIoT devices are password-, token-, or biometrics-secured, protected, and difficult to access, as they can revert to the default device factory settings.

5.1.2 Access control

Access Control is a crucial protection mechanism for the IIoT, granting permissions and privileges to various tools and system applications within the IIoT. Researchers have proposed various access control mechanisms to ensure the security of the IIoT. However, other measures that should be adhered to by the administrators include the following:

1. *Define roles*: To start, it is necessary to identify the various functions existing within the IIoT infrastructure. When creating these roles, it is important to take into account the job duties, responsibilities, and access needs associated with them.
2. *Define permissions within the IIoT infrastructure*: Permissions may be defined as the precise authorizations that are necessary for each position. This entails the identification of the specific tasks and operations that users in each position should possess the capability of executing. This should be applied to all tools and devices within the entire IIoT infrastructure.
3. *Role allocation within the IIoT*: This task involves the allocation of certain roles to particular users, with the criteria for these assignments being determined by their respective work positions and associated obligations. It is paramount to ensure that each user is appropriately assigned to the role(s) that accurately represent their access needs.
4. *Mapping roles within the IIoT*: Role mapping involves the establishment of connections between roles and permissions. The allocation of permissions to certain roles is essential to ensuring that users assigned to a given position are granted the appropriate access privileges. System administrators should be careful while establishing such connections to avoid granting privileges to unauthorized users or the other way around.
5. *Periodic evaluations and updates*: It is important to conduct regular evaluations in order to ascertain that role assignments and permissions are consistently matched with any changes that may occur within the IIoT infrastructure or the entire manufacturing industry at large. Ensure that the appropriate modifications are made to accommodate newly assigned responsibilities or to make necessary adjustments to existing roles as required.

5.1.3 Data security/encryption

Data encryption is a process that involves the transformation of data into a coded form, therefore ensuring its confidentiality and integrity, even in the event of illegal interception of the encrypted data packets during transmission. This approach demonstrates a high level of efficacy in safeguarding data

and guaranteeing its integrity in the face of potential security breaches. In order to ensure the security of data in the IIoT and its services, rigorous encryption techniques and data backup procedures should be implemented (novel techniques can be adopted from those discussed in Sect. 4.3.3). This will mitigate unauthorized access to the data and provide efficient data restoration in the event of unforeseen system failures or data loss. Hence, ensuring data within the entire infrastructure is well secured, both in transit and at rest. However, other important measures that should be observed to enhance data security between the IIoT and its digital services and modules include the following:

1. *Pay attention to sensitive data*: Given that the IIoT deals with a lot of data in transit, which is regarded as very sensitive compared to data at rest, it is crucial that administrators use the chosen strong encryption techniques to safeguard any sensitive data before transferring it. Also, ensure the use of encrypted protocols such as HTTPS, SSL, TLS, FTPS, and others to guarantee the protection of data during transit.
   Meanwhile, to ensure the security of data at rest, it is recommended to use encryption techniques to encrypt important files before their storage or, alternatively, by opting for the encryption of the storage device itself.
2. *Ensure a secure network connection*: To enhance the security of data during transmission in addition to encryption, it is essential to deploy robust network security measures such as firewalls and network access control mechanisms. These network security solutions play a crucial role in safeguarding data transmission networks from potential threats posed by viruses or other unauthorized invasions.
3. *Use preventive security measures*: To ensure precautionary measures on important data for the entire IIoT infrastructure, it is not advisable to depend only on reactive security techniques for the protection of important data. Rather, it is recommended to use proactive security techniques that can detect data that is at risk and execute efficient data protection protocols for both data in transit, data in use, and data at rest. Some of these proactive measures include routine security calibrations on all data transmission channels, devices, and modules.
4. *Ensure user prompts for sensitive data*: Select secure data solutions that include rules and privileges allowing for user prompting, blocking, or automated encryption of sensitive data throughout its transmission. This includes scenarios where files have been attached to email messages, transferred to cloud storage, detachable drives, or any other form of data transfer.
5. *Establish a data categorization policy*: It is important to establish policies that provide an organized strategy for categorizing and classifying all data within the infrastructure, regardless of its location. This will guarantee that suitable measures for data security are consistently implemented when the data is in a static state and that appropriate actions are taken when data identified as vulnerable is accessed, used, or transmitted.
6. *Ensure the use of a trusted, secure, and reliable cloud vendor*: When considering the use of a public, private, or hybrid cloud provider for the purpose of data or application storage, it is imperative to conduct a thorough evaluation of cloud vendors with regards to the security measures they provide. However, it is crucial to note that relying only on the cloud service for data protection is not advisable. Inquiries about the entities with data access, the encryption methods used, and the frequency of data backups are crucial to address.
7. *Ensure the right trade-off balance between security and performance*: The security and performance conundrum are a general challenge that exists in all security domains, and this is an even more serious issue in data security. Whenever an encryption technique is applied to data, it is always possible to experience a reduction in the performance of such data, depending on the system and purpose it is applied to. Therefore, it is crucial that the right protection mechanism be selected for specific data, as this will reduce the impact of such a trade-off.

5.1.4 Tools and device management

The IIoT tools and devices are a huge part of the entire infrastructure, and similar to data, it is essential to ensure that they are also secured from cyber threats. Most IIoT projects [16, 128] are recently adopting the implementation of monitoring tools such as Prometheus [129] and Grafana [130]. However, it is worth noting that these tools are essentially used for the collection of real-time metrics from various system sources in order to ensure the early detection of system errors and other unforeseen issues. Therefore, as a preventive measure, we deem it paramount to propose some guidelines to be followed for the systems, tools, and devices that will be used in the entire IIoT infrastructure.

1. *Use devices with encryption capability*: Ensure that all devices within the IIoT infrastructure can be encrypted. In the event that a device lacks functionality for an encrypted communication channel through wireless connectivity, it is advisable to establish a wired connection instead. Also, if a device lacks the capability to provide encryption, it is advisable to acquire an alternative device or entirely disconnect the device from the network infrastructure.

2. *Ensure correct configurations*: Misconfiguration flaws during device security settings are often overlooked in manufacturing industries, which can be detrimental to the entire infrastructure. It is essential that developers, system administrators, and employees pay close attention to the security configurations of any devices that would be used within the IIoT infrastructure. Ensure that you establish and monitor non-default security settings for devices, including the programs and applications running on them, while removing any unused features, programs, or applications.
3. *Ensure frequent device updates*: In addition to ensuring all devices are correctly configured, it is also crucial to set an automatic patch update on devices as soon as they are released. In the event of a delayed patch release, you must check for updates on a regular basis. Check the manufacturer's website for updates; if updates are no longer offered, consider purchasing a new device. Also, conduct frequent and periodic assessments and audits for missing or outdated patches and possible vulnerabilities in misconfigurations.
4. *Ensure antivirus and firewalls are installed*: When using IIoT tools and devices, it is imperative to safeguard each device within the network, with special attention given to "legacy" systems. This can be achieved by setting up firewalls and antivirus software on all laptops, desktops, and servers. Additionally, tablets and smartphones should be configured with proper security settings, such as two-step authentication, strong passcodes, restricting automatic Wi-Fi connections, and exercising caution when installing new applications.
5. *Adopt factory reset if a malfunction is detected*: If any tool or device connected to the IIoT is noticed to exhibit decreased performance or malfunction, it is a sign of the presence of viruses. Certain types of computer viruses may be stored in the device's memory and can be effectively removed via the simple act of restarting the device. If the device continues to exhibit slowness or unresponsiveness even after a reboot, it is advisable to do a factory reset. Also, when excessive internet use or billing costs are noticed, this may indicate a potential hijack of a device. The adoption of factory and passcode reset procedures should solve this issue.
6. *Ensure adequate management of all tools and devices in the IIoT*: Attackers use various devices, including routers, switches, and endpoints, to get unauthorized access to industrial data and applications. They do this by exploiting vulnerable ports, excessively permissive network traffic rules, and hardware that has not been sufficiently patched or maintained. Therefore, it is essential to ensure that all these negligence are carefully mitigated during device and system installations and updates.
7. *Ensure the removal of unused features*: It is imperative that all features that are no longer needed within the IIoT tools and applications be removed as soon as possible. Failure to eliminate unnecessary features and components exposes the application to vulnerabilities. This, in turn, creates an opportunity for attackers to exploit the application using techniques like code injection, whereby malicious code is inserted and then executed by the application. Table 5 provides a summary of the outlined guidelines and completion indicative measures that should be considered in the further course of deploying an IIoT ecosystem with regards to the security of digital services and modules within the infrastructure.

5.2 Guide to secure network interconnectivity

Secure network connectivity is considered pivotal to achieving profound protection in any security domain, let alone in cybersecurity. Therefore, considering the interconnectivity nature of the IIoT infrastructure, it is crucial to ensure that the network connections between different components of the IIoT are secured. This section provides guidelines on practical implementations that ensure the security of the entire IIoT network interconnectivity.

5.2.1 Network segmentation

One of the crucial steps of securing heterogeneous network connections is through network segmentation. Network segmentation refers to the procedure of partitioning expansive networks into smaller sub-networks in order to restrict traffic flow across various regions to prevent the spread of malware. Such compartmentalization enables network administrators to effectively modify security regulations with enhanced accuracy. The implementation of such segmentation within the IIoT will serve as a preventive measure for network attack mitigation while significantly contributing to the development of detailed security procedures and the establishment of security rules based on contextual factors.

Moreover, once the network has been partitioned, the process of establishing monitoring capabilities, identifying network inefficiencies, and improving its security is significantly facilitated. Therefore, it is important that the given network segmentation guidelines are adhered to within the entire IIoT infrastructure.

1. *Identify and classify asset values*: Prior to initiating any network segmentation procedures, it is essential for the IIoT developers to conduct an inventory of all components, such as databases, cobots, tools, devices,

Table 5 Summary of guides to secure digital services and modules with completion indicators

Guide to secure digital services and modules		Completion indicators
Authentication	Modify default system settings	Multi-factor authentication is required to access systems within the entire IIoT infrastructure
	Avoid using the same logins	
	Ensure devices and credentials are not hard-coded	
	Adopt a good authentication mechanism	
	Frequent password update	
	Ensure default hardware reset devices are protected	
Access control	Define roles	Permissions are granted to only authorized users and denied to unauthorized users within the entire IIoT
	Define permissions within the IIoT structure	
	Role's allocation within the IIoT	
	Mapping roles within the IIoT	
	Periodic evaluations and updates	
Data security	Pay attention to sensitive data	Entire IIoT data is secured against any form of cyber and physical threats
	Ensure a secure network connection	
	Use preventive security measures	
	Ensure user prompts for sensitive data	
	Establish a data categorization policy	
	Ensure the use of a trusted, secure, and reliable cloud vendor	
	Ensure the right trade-off balance between security and performance	
Tools and device management	Use devices with encryption capability	Tools and devices within the entire IIoT infrastructure are protected against cyber and physical attacks
	Ensure correct configurations	
	Ensure frequent device updates	
	Ensure antivirus and firewalls are installed	
	Adopt factory reset if a malfunction is detected	
	Ensure adequate management of all tools and devices in the IIoT	
	Ensure the removal of unused features	

sensors, cameras, etc., and allocate corresponding values to them. It is important to arrange each item based on their respective levels of significance and sensitivity. These categorizations will afterwards serve the purpose of defining the different zones of trust within the IIoT network.

2. *Merge relevant network resources*: After completing the documentation of different items, the next phase involves defining categories of similar network resources. Items with lower security levels should be consolidated within a single network, while those with higher security levels should be allocated to a separate network. As the network architecture takes shape, the IIoT can implement enhanced security measures on networks containing more critical data in order to ensure protection.
3. *Ensure the mapping of data flows throughout the network*: Since network segmentation enhances network security by isolating network segments, the mapping of data flows across such segments makes it more difficult for an intruder to penetrate the network even after gaining an initial access. Hence, such mapping strategy should be adopted in the entire IIoT to enhance the security of the network connection. However, it is important to do a comprehensive mapping of data flows across all systems inside the network, including the following:
   - *North-bound traffic*: The traffic that goes out of the IIoT network. Such as employees using managed devices connected to the IIoT network to access external domains.

- *East–west traffic*: The traffic between systems within the network perimeter, such as a front-end webserver and a back-end database server in the IIoT's data center network.
- *South-bound traffic*: The traffic that consists of data entering a network segment, such as staffs or clients accessing the IIoT's intranet web server.

4. *Ensure the deployment of segmentation gateway*: Establishing segment boundaries is essential not only for assuring network security for the infrastructure, but also for making well-informed decisions using the network traffic. To enforce access controls on each network segment in the entire IIoT, a segment gateway must be deployed to guarantee that all network traffic entering and leaving the segment must pass through the gateway. As a consequence, the IIoT may need multiple gateways to implement effective segmentation. However, considering the significance of such gateways in achieving the required network protection, IIoT can utilize virtual firewall to cut down costs.
5. *Ensure the segregation of IIoT devices from the rest of the network*: With the roll-out of IPv6, the scalability of IoT networks is practically limitless. Therefore, all devices connecting to the IIoT must be isolated from the rest of the network to prevent direct access. The network engineers might require distinct network cabling and switches, or alternatively, private VLANs, to safeguard against attacks to logical networks of similar devices. Another possible approach is using a set of designated IP addresses or employing Network Address Translation (NAT) techniques to allow for the restriction and supervision of network traffic via the administrative interface. Tools such as Prometheus and Grafana can be utilized for such monitoring while dedicated routers handle the restriction.
6. *Beware of excessive or inadequate segmentation*: When implementing network segmentation, it is prevalent to over segment into too many networks or under segment into too few networks. If each network segment is not properly managed, over-segmentation can force staffers to pass through multiple access points in order to gain access to data, causing workflow delays and constraining traffic flow, as well as increasing security risks. Meanwhile, under-segmenting a network can also be inefficient if there is too little distance between each system, because two or three segments of a single network would not provide the necessary level of security for network segmentation. In an ideal situation, there should be a balance between having sufficient resources to monitor and manage several networks without compromising security or employee productivity.
7. *Adhere to the privilege of least principle*: After the successful implementation of network segmentation, it is imperative that each network within the IIoT adhere to the zero-trust model and the concept of least privilege. These practices entail restricting network access at all levels, necessitating that all entities inside the network boundaries, whether internal or external, undergo authentication and verification prior to being granted access to further segments of the network. With zero trust, the administrator can promptly detect and identify any malicious actors or unauthorized entities trying to breach the networks, thus granting only authorized users the appropriate permission to access a specific network segment.

5.2.2 Network monitoring

Network monitoring plays an integral role in the IIoT network by monitoring and assessing the performance and resilience of the network. The IIoT network is assumed to include sensors and monitoring points strategically positioned at critical sites, such as servers, firewalls, routers, etc., inside the network infrastructure to effectively record real-time data. Such data is further analyzed and used for different purposes. Some important guidelines to be adhered to for efficient IIoT network monitoring include the following:

1. *Frequently monitor segmented networks*: To order to maintain the integrity of the IIoT network infrastructure, it is essential that segmentation procedures include ongoing monitoring of the network traffic and performance to mitigate any potential gaps or vulnerabilities. IIoT network administrators should ensure regular network risk assessments and penetration testing. This plays a crucial role in the identification of security vulnerabilities that need prompt mitigation.
2. *Adopt frequent auditing of segmented networks*: Periodic network audits are of crucial significance as they provide the IIoT infrastructure with the opportunity to reassess the efficacy of their existing security practices. Updates to the network segmentation plan may be necessary due to the introduction of new users, processes, operations, or industrial requirements over time. It is ideal to perform such audits on a yearly basis.
3. *Ensure packet filtering*: By monitoring incoming network traffic, the IIoT ecosystem can adopt techniques that mitigate attacks such as DoS. These techniques include filtering traffic originating from a particular IP address, imposing limitations on the number of packets that can be transferred from a single IP address, and redirecting or discarding packets from designated IP addresses before they can reach their intended destination.

4. *Keep an eye on network devices*: Despite the monitoring and auditing of the network itself, it is imperative to also monitor the network devices within the entire IIoT infrastructure such as routers, switches, firewalls, load balancers, and wireless access points. The objective of monitoring these devices is to ensure that the network is operating effectively and performing to the expected standards while ensuring security. It also helps the network administrators proactively detect issues and take appropriate measures to maintain a reliable and secure network infrastructure. In the event that certain devices are not in use, consider switching them off or disconnecting them from the power source.
5. *Monitor the baseline network behaviour*: To proactively detect possible issues, it is essential for the IIoT network administrator to possess an in-depth grasp of the network's baseline performance. By observing and analyzing network behavior over an extended period, ranging from a few weeks to several months, network administrators can gain insights into the typical patterns and characteristics of network activity. This process enables administrators to establish a reference point for normal network behavior, thus setting up threshold values for the purpose of generating alerts once there is a change in network activity.
6. *Implement reports at each layer*: Networks operate according to the OSI model, whereby every communication inside a network entails the transmission of data between systems through many end points, devices, and connections. Every component inside the network plays a role in facilitating data transfer operations at certain levels. For instance, cables at the physical layer, IP addresses at the network layer, transport protocols at the transport layer, etc. The failure of a data connection can occur at any of these layers or even at multiple points. Therefore, it is essential for the IIoT to utilize a monitoring system that allows different technologies to monitor at all network layers as well as various types of network devices that would facilitate problem detection and resolution, such that whenever an issue is detected, the monitoring system can easily pinpoint where the issue comes from.
7. *Implement high reliability monitoring system with flexible failover*: Most monitoring systems are installed within the monitored network. This expedites and improves the data collection from monitored devices. Nonetheless, if a problem occurs and the network fails, the monitoring system may also fail, rendering all the collected monitoring data inaccessible or unusable for analysis. Therefore, it is encouraged that the IIoT implement a monitoring strategy with high reliability without failover. High reliability and availability assure that the monitoring system does not have a single point of failure; therefore, even if the entire network goes down, the monitoring system is still accessible, allowing the network engineer to detect and resolve issues.

5.2.3 Network configurations

Similar to network monitoring, the importance of having the right network configurations for the IIoT infrastructure cannot be overemphasized, as network configuration is essential for the industry's operations, IT efficiency, and connectivity while sustaining network traffic, ensuring security, eliminating disruptions, and maintaining stability. While network monitoring focuses on collecting and analyzing data on network functionality and performance, network configurations proactively focus on configuring and managing network devices and services. Important guidelines that must be followed for efficient IIoT network configuration are as follows:

1. *In-depth understanding of the network architecture*: First, a comprehensive knowledge of the IIoT 's network architecture and configuration, as well as the interconnected devices and their functional integration, is required. Additionally, it's crucial to have a complete inventory of all network equipment, including servers, firewalls, routers, and switches, as well as a network map that fully describes the software, hardware, systems, and devices present in the network. All these will give profound insight to the network engineers and administrators on how to better approach performance and security for the network infrastructure.
2. *Ensure standardized configuration of devices*: To mitigate the risk of human error or other configuration problems during the installation of new devices, it is advisable to establish standardized settings for each category of device inside the IIoT network. This includes routers, switches, network topology, and other relevant components. By implementing such standardized configurations, we can ensure consistency and minimize the likelihood of misconfigurations or other operational issues when deploying new devices. Network configuration management software is an effective method for achieving this objective.
3. *Keep track of and record changes*: It is advisable to monitor and record incidents of configuration modifications within the IIoT network infrastructure while establishing a system of notifications to promptly warn relevant parties upon their occurrence. It is also crucial to follow up with comprehensive backups of all network modifications to facilitate subsequent inspection in the event of errors and to enable the restoration of earlier settings if deemed essential.

4. *Automate where necessary*: The automation of operations within the IIoT network devices that would otherwise need human involvement has the potential to mitigate the occurrence of human errors, facilitate teams in managing repetitive tasks, oversee configuration changes across several devices, and ensure adherence to regulatory requirements.
5. *Ensure redundancy in your structure*: Regardless of the level of preparedness, network components have the potential to experience failures (due to security breaches or otherwise), resulting in a complete interruption of operations. It is essential to mitigate possible catastrophes by implementing redundancy within the IIoT's network infrastructure, thereby ensuring the continuity of network operations in the event of device malfunction.
6. *Ensure a centralized configuration management*: It is highly likely that the IIoT development might be allocated a significant portion of resources towards network management activities, a substantial proportion of which are characterized by manual execution and repetitive in nature. Therefore, the adoption of a centralized network management technique will result in significant time and cost savings.
   As such, the use of integrated network management procedures and tools will enable the administrators to remotely update and configure hardware while also facilitating the total automation of several simple processes. Hence, ensuring that minor configuration errors that might lead to network downtime, data loss, and other security issues are mitigated [131]. Table 6 provides a summary of the outlined guidelines and completion indicative measures that should be considered in the further course of deploying an IIoT infrastructure with regards to securing network interconnectivity within the infrastructure.

5.3 Guide to secure cloud database

With the wide adoption of smart devices in the manufacturing domain, the accumulation of huge data has never been easy, and so has the adoption of third-party cloud services for storing such data, which eventually comes with enormous security and privacy risks. Although these technologies provide notable benefits in terms of scalability and accessibility, they also present distinct security concerns that cannot be overlooked, as well as devastating consequences that must be effectively mitigated in order to safeguard sensitive data. Therefore, it is essential that the IIoT's infrastructure cloud database remains secure.

5.3.1 Cloud database

The guidelines outlined in Sects. 5.2.1, 5.2.2, and 5.2.3 encompass essential elements that contribute significantly to the security of the IIoT infrastructure. These elements include network security tools that safeguard the communication channel between the cloud database and other services, data security techniques that encrypt sensitive data both in transit and at rest, strong authentication, and access control to the cloud database, among others. Other specific guidelines that are not covered in the aforementioned sections include the following:

1. *Ensure a limited access of IIoT database to third-party cloud vendors*: In case the IIoT team decides to indulge in the services of any third-party cloud vendors, it is very important they understand that even after ensuring the use of a trusted, secure, and reliable cloud vendor (as highlighted under the guidelines of data security), it is also crucial to ensure that they have full access control of the database themselves rather than the cloud provider. By so doing, they can decide whether or not to grant any access to the provider, and if they do, it should only be limited to the requirements and the period of time the permission should last.
2. *Ensure the frequent monitoring of database activities*: Consistent monitoring of database activity is an essential element in understanding data operations with respect to user activity and system functionalities in order to identify abnormalities in the IIoT database. Consequently, frequent monitoring facilitates the early detection of possible risks, hence allowing rapid response measures.
3. *Ensure the frequent auditing of database activities*: Auditing serves to document the activities undertaken by both systems and users, enabling a comprehensive investigation of any possible incidents. The combined practices of auditing and monitoring the IIoT cloud database will offer a complete perspective on database activity and make a substantial contribution to enhancing its security.
4. *Ensure frequent database software updates*: As any database can be susceptible to cyber threats, so can the database software, since adversaries are continuously in search of vulnerabilities to leverage. Therefore, to ensure the security of the IIoT cloud database, it is crucial to consistently update and apply patches where needed to the database software, especially in instances where the IIoT platform team may choose to host their own database in a cloud environment or use a modified variant of a cloud-based database solution.
5. *Ensure database servers are separated from other servers*: In an event that the IIoT teams decides to host its own database, it is important that database servers are

Table 6 Summary of guides to secure network interconnectivity with completion indicators

Guide to secure network interconnectivity		Completion indicators
Network segmentation	Identify and classify asset values	The entire IIoT network is mapped and segmented between critical systems and devices
	Merge relevant network resources	
	Ensure the mapping of data flows throughout the network	
	Ensure the deployment of segmentation gateway	
	Ensure the segregation of IIoT devices from the rest of the network	
	Beware of excessive or inadequate segmentation	
	Adhere to the privilege of least principle	
Network monitoring	Frequently monitor segmented networks	The entire segmented IIoT network is monitored, and audits are recorded accordingly
	Adopt frequent auditing of segmented networks:	
	Ensure packet filtering	
	Keep an eye on network devices	
	Monitor the baseline network behaviour	
	Implement reports at each layer	
	Implement high reliability monitoring system with flexible failover	
Network configurations	In-depth understanding of the network architecture	Entire IIoT tools and device network configurations are standardized and centralized
	Ensure standardized configuration of devices	
	Keep track of and record changes	
	Automate where necessary	
	Ensure redundancy in your structure	
	Ensure a centralized configuration management	

situated on an entirely separate host from other servers meant for services such as web, applications, or networks. This will help to reduce the risk of unauthorized users gaining access to the IIoT database.

6. *Ensure authentication and access control are implemented on the IIoT database servers*: In line with the guidelines for data security, it is important to reiterate the importance of authentication and access control for not just the data itself but also the database storing the data, considering those protection techniques are the first crucial steps in ensuring secure access to cloud databases.

In addition, the IIoT team should make sure that the principle of first privilege is strictly adhered to, such that access privileges are only permitted to those who require them and only to the extent required. Moreover, authentication should not solely depend on passwords but also utilize a blend of various authentication methods (multi-factor), such as passwords, tokens, and biometrics.

5.4 Guide to data privacy

Data privacy is a specific aspect of data security that focuses on the proper management of personal data in accordance with data protection laws, regulations, and established privacy policies such as EU GDPR [132, 133], CCPA [134], and IIC [135]. Ensuring data privacy in the IIoT entails implementing effective data management practices to protect against unauthorized entities. These data include the user's information, operational data, and audit data while in transit, at rest, or in use. Ensuring data privacy should be a paramount concern for manufacturing industries, given the heterogeneous IT and OT data shared within the IIoT ecosystem. Moreover, non-compliance with data privacy standards in such a scenario can result in significant financial, operational, and reputational consequences.

The EU General Data Protection Regulations [133] have effectively established robust data privacy legislation that bestows upon users a comprehensive array of entitlements on how their data should be managed. These include the right to:

1. Provide informed consent regarding the usage of their data,
2. have their inaccurate data rectified,
3. have their data completely erased,
4. have clear limitations on the processing of their data,
5. have the option to transfer their data to another entity, and
6. have the right to object to the processing of their data in response to changing circumstances.

Despite the extensive coverage of data privacy in various domains under the aforementioned regulations and those covered in Sect. 2, it is crucial to emphasize additional privacy guidelines that are specific to the manufacturing sector. These guidelines can be applied to both industries and users alike.

5.4.1 Data privacy guides to industries

As earlier highlighted, data privacy is undoubtedly linked to data security in various facets of ensuring data protection within the IIoT. Therefore, most data privacy policies for the IIoT work in tandem with those for data security. These guidelines include the following:

1. *Ensure data security and privacy awareness*: Providing comprehensive training on data security and privacy approaches to all employees within your industry is essential. It is advisable to incorporate data privacy training into the overall training program as well as the induction procedure for newly hired personnel.
2. *Enact the zero-trust strategy*: The Zero Trust approach limits network access by isolating systems and segmenting network access according to user privileges and authentication. This strategy ensures seamless execution of regulations and protection measures for all users, devices, systems, and data, irrespective of their connection location. The philosophy of 'trust but verify' is crucial for enterprises in today's world.
3. *Utilize the available security tools*: Industries should provide security tools for all employees and ensure that they are being used as instructed. These include password managers, VPNs, encryption solutions, etc. These tools will help significantly reduce the susceptibility to cyber threats.
4. *Observe network behavior for any suspicious activity*: We cannot stress enough the importance of monitoring and segmentation the industrial network, as this is the ideal way to ensure early detection of threats, thereby drastically reducing or mitigating any unforeseen compromise.
5. *Do not undervalue the curiosity of hackers*: Different attackers have different motives regarding their exploit and the data they wish to gain access to. Therefore, whether the industry is just a startup or a Fortune 500 company, it is essential to ensure data security and privacy are strictly upheld.

5.4.2 Data privacy guides to users

As a user or client, you have little influence over the storage and privacy measures used by industries to safeguard your data. However, there are some simple measures you can take to enhance the privacy of your data. It is advisable to acquaint yourself with the various privacy tools as a first step. At the very least, it is necessary to use a VPN to encrypt your internet connection, as well as employ a trusted password manager to enhance the security of your online accounts.

1. *Ensure frequent data backup*: In the event of a data breach, maintaining a safe backup will greatly increase the likelihood of retaining your data.
2. *Exercise caution while using IIoT devices*: Be wary of connecting to IIoT devices with outdated firmware as they are mostly spyware breeders. The significance of ensuring all IIoT devices are always updated cannot be overemphasized.
3. *Adopt multifactor authentication mechanisms*: Enable multi-factor authentication to enhance security and privacy while preventing unauthorized access to critical accounts in the event of password compromise. Give priority to using multi-factor authentication mechanisms that do not rely on SMS.
4. *Remain vigilant to unusual queries*: Be cautious of any attention-grabbing clickbait material or any other suspicious content.

In order to ensure strict follow-through and implementation of the guidelines covered in this section, different measures can be taken to make sure the procedures and security mechanisms are applied and understood throughout a project. Table 7 provides a summary of the outlined guidelines and completion indicative measures for secure cloud databases and data privacy that should be taken into consideration during the IIoT deployment process.

6 Challenges and open issues

IIoT continues to face significant challenges in the domain of cybersecurity. Fault infrastructural design and severe industrial settings may have a negative impact on network connectivity and the ability to transmit data. Furthermore, the fluctuating industrial environmental circumstances and interfering elements may lead to a compromise in the quality

Table 7 Summary of guides to secure cloud databases with completion indicators

Guide to secure cloud database and data privacy		Completion indicators
Cloud database	Ensure limited access of IIoT databases to third-party cloud vendors	The IIoT cloud database is fully protected. It is regularly monitored, and audits are recorded accordingly
	Ensure the frequent monitoring of database activities	
	Ensure the frequent auditing of database activities	
	Ensure frequent database software updates	
	Ensure database servers are separated from other servers	
	Ensure authentication and access control are implemented on the IIoT database servers	
Data Privacy	Privacy to industries	
	Ensure data security and privacy awareness	The entire IIoT ecosystem ensures privacy for both operational data and user data
	Enact the zero-trust strategy	
	Utilize the available security tools	
	Observe network behavior for any suspicious activity	
	Do not undervalue the curiosity of hackers	
	Privacy to users	
	Ensure frequent data backup	
	Exercise caution while using IIoT devices	
	Adopt multifactor authentication mechanisms	
	Remain vigilant to unusual queries	

of service. Therefore, ensuring seamless data transfer without any delays is crucial to ensure real-time compliance, as the generated data is often time sensitive. Likewise, it is also essential to guarantee that the efficient process of industrial automation can endure the constraints posed by the limited storage capacity of sensors and their computational energy reserves. Also, it is important to consider efficient resource management approaches that allow for data transfer without impacting the computational efficiency and storage of the sensors. The following are some of the major challenges and open issues in IIoT for smart manufacturing:

6.1 Security and privacy

The IIoT has always prioritized security and privacy due to the need for robust measures to provide high levels of protection, minimal delays, exceptional dependability, efficient energy use, and expansive connections. Integrating the legacy systems of the IIoT with the internet will facilitate the connection of many kinds of industrial equipment to publicly accessible services. However, this integration would raise several security and privacy concerns. In the event of a network breach, the whole industrial infrastructure would be vulnerable to severe risks. Therefore, it is important to evaluate the security of particular physical devices, tools, applications, software, and embedded operating systems. Even though the recent advancements in deep learning, blockchain technology, and federated learning have immense potential to ensure the security and privacy of the IIoT, these techniques are still in their infancy stages.

Furthermore, the premise of most novel IIoT infrastructural design techniques heavily emphasizes automation. However, implementing self-configuration and automation might potentially reveal weaknesses that could be exploited by an attacker to breach the system. Also, the incorporation of cloud technology into industrial systems will result in concerns about data privacy. These concerns may be mitigated by implementing strategies that include guides and novel protection mechanisms for the time being, considering the evolution the IIoT ecosystem usually goes through. In addition, network security vulnerabilities, such as the absence of adequate security measures for network protocols like TCP, UDP, Modbus, etc., may result in unauthorized access, data breaches, DDoS attacks, and data manipulation. Currently, there is a scarcity of documented research on security and privacy for the IIoT, with the majority of suggested security and privacy frameworks being in their early stages of development.

Moreover, given the complexity of the IIoT ecosystem, most of the techniques proposed by the research community focus on just one or two security issues within the entire ecosystem. As such, the need for an end-to-end security and privacy protection mechanism can never be overemphasized. Therefore, addressing all IIoT security and privacy

challenges in one fell swoop still remains a major challenge for the security experts and research community as a whole.

6.2 Interoperability and scalability

Achieving scalability and interoperability is a critical area of research for the IIoT, given the diverse array of components that comprise the industrial environment. IIoT architectures should be created with the capability to readily adjust or expand in order to support a large number of devices. Every procedure implemented for executing data analytics and algorithms must be capable of scaling up as the infrastructure expands [136]. The variety and complexity of IIoT, as well as the many connections and technologies used, will result in scaling challenges. Research indicates that the incorporation of edge computing, fog computing, SDN, deep learning, and blockchain technology only aggravates the challenges related to interoperability and scalability in the context of the IIoT [10]. Although the incorporation of AI with these technologies is a current prospect for solving this research problem, it still leaves a big loophole before readily available solutions are implemented.

6.3 Resource limitations

The heterogeneous nature of IIoT devices, in general, has led to an unregulated limitation of resources in terms of processing power, memory capacity, and energy consumption. In the IoT ecosystem, there is a need for sufficient computing and storage capabilities to transform data into actionable insights. Certain applications prioritize low latency, whereas others, such as those involving archival data and time series analysis, need intricate processing. Effective management of these resources is crucial due to the specified constraints. Relevant improvements in the heterogeneity of IIoT architecture or adjustments to specific protocols may be used to regulate IIoT resources. An alternative strategy involves the integration of further novel advancements in machine learning and AI, which could serve as a fundamental remedy. Existing approaches such as [137, 138], and [139] have proposed different strategies to help reduce the computational burden associated with IIoT resources; however, there is still more work to be done in order to fully mitigate such a challenge.

6.4 Decentralization

Another potential area of future research is the transition from a centralized to a decentralized model for IIoT environments. At present, the majority of IIoT use cases function in a centralized fashion. Nevertheless, the transition from a centralized to a decentralized distribution model has recently been noticed [140–143] due to the security, reliability, and performance advantages of the latter.

With an existing trusted decentralized ecosystem, the likelihood of detecting a threat is increased, while the risk of cyberattacks is reduced due to the distributed nature of the IIoT. Decentralized edge and fog computing solutions are increasingly becoming popular due to factors such as infrastructure, network availability, bandwidth limits, latency, and the need for high computing power. Decentralized peripheral network administration is exceptionally efficient, and its integration with SDN may improve its performance. However, the development of a decentralized architecture that is universally applicable to all industrial settings is a formidable undertaking because it can lead to the compromise of several industries simultaneously. In order to facilitate efficient coordination and collaboration among a diverse array of heterogeneous nodes comprising different decentralized architectures, robust methods and mechanisms will be necessary [144].

7 Conclusions

The increased adoption of IIoT has boosted the economic sector of the manufacturing industry while presenting new cyber security challenges. This paper provides an in-depth discussion and analysis of the guides and recent defense mechanisms that would aid with the adoption and deployment of secure and privacy-preserving IIoT in smart manufacturing. The survey first examined the different guides, standards, and policies proposed by different organizations, agencies, and academia. It then draws insights and provide guidelines suitable for the IIoT infrastructure in the manufacturing domain. The guidelines ensure easy adoption and deployment of the different facets of the protection mechanisms, which are covered in greater depth. In terms of the IIoT architectural overview, a brief discussion of the four-layered model is provided while delineating each layer of the architecture. Additionally, possible IIoT attacks, including those that emanate due to the IT/OT convergence, are provided, followed by an in-depth discussion and analysis of the different defense mechanisms that would mitigate such attacks. Finally, we examined the challenges and open questions in relation to technologies that are vital and necessary for an efficient, secure, and privacy-preserving IIoT ecosystem in smart manufacturing.

Future work will investigate the importance of cybersecurity in industrial digital twins, thereby proposing strategies for ensuring a secure and privacy-preserving digital twin in smart manufacturing.

Author contribution S.M.A. made substantial contributions to the conception or design of the work. He also drafted the work and revised it

critically for important intellectual content. S. L. M. revised the work critically for important intellectual content. She is in charge of the funding acquisition and approval of this version for publication. S.M.A. and S. L. M. both agree to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately resolved.

Funding Open access funding provided by University of Southern Denmark. This project is part of the funding received from the ONE4ALL project funded by the European Commission, Horizon Europe Programme under the Grant Agreement No. 101091877.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no competing interests.

References

1. Khan, W.Z., Rehman, M.H., Zangoti, H.M., Afzal, M.K., Armi, N., Salah, K.: Industrial internet of things: recent advances, enabling technologies and open challenges. Comput. Electrical Eng. **81**, 106522 (2020)
2. Mekala, S.H., Baig, Z., Anwar, A., Zeadally, S.: Cybersecurity for Industrial IoT (IIoT): threats, countermeasures, challenges and future directions. Comput. Commun. **208**, 294–320 (2023). https://doi.org/10.1016/j.comcom.2023.06.020
3. Sinha, S.: State of IoT 2023. IoT Analytics. https://iot-analytics.com/number-connected-iot-devices/ (accessed October 2023.
4. Shoploigx. "Top IIoT Statistics for 2020." Shoploigx Smart Factory. https://shoplogix.com/top-iiot-statistics-for-2020-head-into-the-year-with-20-20-vision/ accessed October 2023.
5. Technologies, N. G.: Industrial Internet of Things Market Size, Share & Trends Analysis Report " Grand View Research. https://www.grandviewresearch.com/industry-analysis/industrial-internet-of-things-iiot-market accessed October 2023.
6. Abdullahi, S. M., and Lazarova-Molnar, S.: Cybersecurity in distributed industrial digital twins: threats, defenses, and key takeaways," presented at the 1st international workshop on distributed digital twins, Groningen, The Netherlands, (2024)
7. Abdullahi, S. M., and Lazarova-Molnar, S.: Toward a Unified Security Framework for Digital Twin Architectures," In: *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2–4 pp. 612–617, (2024) https://doi.org/10.1109/CSR61664.2024.10679442.
8. Mahesh, P., et al.: A Survey of cybersecurity of digital manufacturing. Proc. IEEE **109**(4), 495–516 (2021). https://doi.org/10.1109/JPROC.2020.3032074
9. Phuyal, S., Bista, D., Bista, R.: Challenges, opportunities and future directions of smart manufacturing: a state of art review. Sustain. Futur **2**, 100023 (2020). https://doi.org/10.1016/j.sftr.2020.100023
10. Alabadi, M., Habbal, A., Wei, X.: Industrial internet of things: requirements, architecture, challenges, and future research directions. IEEE Access **10**, 66374–66400 (2022). https://doi.org/10.1109/ACCESS.2022.3185049
11. Franco, J., Aris, A., Canberk, B., Uluagac, A.S.: A Survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems. IEEE Commun. Surv. & Tutorials **23**(4), 2351–2383 (2021). https://doi.org/10.1109/COMST.2021.3106669
12. Wu, Y., Dai, H.N., Wang, H., Xiong, Z., Guo, S.: A Survey of intelligent network slicing management for industrial IoT: integrated approaches for smart transportation, smart energy, and smart factory. IEEE Commun. Surv. & Tutorials **24**(2), 1175–1211 (2022). https://doi.org/10.1109/COMST.2022.3158270
13. Shi, Z., Xie, Y., Xue, W., Chen, Y., Fu, L., Xu, X.: Smart factory in Industry 4.0. Syst. Res. Behav. Sci. **37**(4), 607–617 (2020). https://doi.org/10.1002/sres.2704
14. Yu, X., and Guo, H.: A Survey on IIoT Security, in *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*, 28–30, pp. 1–5, (2019) https://doi.org/10.1109/VTS-APWCS.2019.8851679.
15. Tange, K., Donno, M.D., Fafoutis, X., Dragoni, N.: A systematic survey of industrial internet of things security: requirements and fog computing opportunities. IEEE Commun. Surv. & Tutorials **22**(4), 2489–2520 (2020). https://doi.org/10.1109/COMST.2020.3011208
16. Bravos, G., et al.: Cybersecurity for industrial internet of things: architecture, models and lessons learned. IEEE Access **10**, 124747–124765 (2022). https://doi.org/10.1109/ACCESS.2022.3225074
17. Panchal, A. C., Khadse, V. M., and Mahalle, P. N.: Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures," In: 2018 IEEE global conference on wireless computing and networking (GCWCN), 23–24, pp. 124–130, (2018) https://doi.org/10.1109/GCWCN.2018.8668630.
18. Elhabashy, A.E., Wells, L.J., Camelio, J.A.: "Cyber-physical security research efforts in manufacturing – a literature review. Procedia Manuf. **34**, 921–931 (2019). https://doi.org/10.1016/j.promfg.2019.06.115
19. DeSmit, Z., Elhabashy, A.E., Wells, L.J., Camelio, J.A.: Cyber-physical vulnerability assessment in manufacturing systems. Procedia Manuf. **5**, 1060–1074 (2016). https://doi.org/10.1016/j.promfg.2016.08.075
20. Chhetri, S. R., Rashid, N., Faezi, S., and Faruque, M. A. A.: Security trends and advances in manufacturing systems in the era of industry 4.0, In: 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 13–16, pp. 1039–1046, (2017) https://doi.org/10.1109/ICCAD.2017.8203896.
21. Shah, Y., and Sengupta, S.: A survey on classification of cyber-attacks on IoT and IIoT devices," in 2020 11th IEEE Annual ubiquitous computing, electronics & mobile communication conference (UEMCON), 28–31, pp. 0406–0413, (2020) https://doi.org/10.1109/UEMCON51285.2020.9298138.
22. Sezgin, A., and Boyacı, A.: A Survey of privacy and security challenges in industrial settings, In 2023 11th International symposium on digital forensics and security (ISDFS), 11–12, pp. 1–7, (2023) https://doi.org/10.1109/ISDFS58141.2023.10131858.
23. Jayalaxmi, P., Saha, R., Kumar, G., Kumar, N., Kim, T.H.: A taxonomy of security issues in industrial internet-of-things: scoping review for existing solutions, future implications, and research challenges. IEEE Access **9**, 25344–25359 (2021). https://doi.org/10.1109/ACCESS.2021.3057766

24. Fagan, M., Megas, K. N., Scarfone, K., and Smith, M.: IoT device cybersecurity capability core baseline, In: "NIST," https://csrc.nist.gov/pubs/ir/8259/a/final, 2020. Accessed: (2023).
25. NIST, The NIST Cybersecurity Framework 2.0, https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd, 2023. Accessed: (2023).
26. ENISA, Baseline Security Recommendations for IoT," in "The Context of Critical Information Infrastructures," ENISA, 2017. Accessed: (2023). [Online]. Available: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
27. ENISA, Guidelines for Securing the Internet of Things," in "Secure supply chain for IoT," ENISA, 2020. Accessed: Sep 2023. [Online]. Available: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things
28. ETSI, Cyber Security for Consumer Internet of Things: Baseline Requirements , https://www.etsi.org/technologies/consumer-iot-security, 2020. Accessed: Sep 2023. [Online]. Available: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
29. ETSI, Guide to Cyber Security for Consumer Internet of Things, https://www.etsi.org/deliver/etsi_tr/103600_103699/103621/01.02.01_60/tr_103621v010201p.pdf, 2022. Accessed: Sep 2023.
30. ISO/IEC, Cybersecurity, In: IoT security and privacy — Guidelines, https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27400:ed-1:v1:en, 2022. Accessed: Sep 2022.
31. CISA, Critical Manufacturing Sector, In: "Cybersecurity Framework Implementation Guidance," https://www.cisa.gov/resources-tools/resources/critical-manufacturing-sector-cybersecurity-framework-implementation, 2021. Accessed: Sep 2023.
32. Ghazaani, S.J., Faulks, M., Pournouri, S.: Secure Deployment of IOT Devices. In: Jahankhani, H., Kilpin, D.V., Kendzierskyj, S. (eds.) Blockchain and Other Emerging Technologies for Digital Business Strategies, pp. 271–316. Springer, Cham (2022)
33. Swessi, D., Idoudi, H.: A survey on internet-of-things security: threats and emerging countermeasures. Wirel. Personal Commun. **124**(2), 1557–1592 (2022). https://doi.org/10.1007/s11277-021-09420-0
34. ElMamy, S.B., Mrabet, H., Gharbi, H., Jemai, A., Trentesaux, D.: A survey on the usage of blockchain technology for cyber-threats in the context of industry 4.0. Sustainability **12**(21), 9179 (2020)
35. Leng, J., et al.: Blockchain-secured smart manufacturing in industry 4.0: a survey. IEEE Trans. Syst. Man Cybern. Syst. **51**(1), 237–252 (2021). https://doi.org/10.1109/TSMC.2020.3040789
36. Rathee, G., Kerrache, C.A., Lahby, M.: TrustBlkSys: a trusted and blockchained cybersecure system for IIoT. IEEE Trans. Industr. Inf. **19**(2), 1592–1599 (2023). https://doi.org/10.1109/TII.2022.3182984
37. Maleh, Y., Lakkineni, S., Tawalbeh, L.A., AbdEl-Latif, A.A.: Blockchain for Cyber-Physical Systems: Challenges and Applications. In: Maleh, Y., Tawalbeh, L.A., Motahhir, S., Hafid, A.S. (eds.) Advances in Blockchain Technology for Cyber Physical Systems. Springer, Cham (2022)
38. Pourrahmani, H., Yavarinasab, A., Monazzah, A.M.H., Van herle, J.: A review of the security vulnerabilities and countermeasures in the internet of things solutions: a bright future for the blockchain. Int. Things **23**, 100888 (2023). https://doi.org/10.1016/j.iot.2023.100888
39. Leng, J., et al.: Blockchain-empowered sustainable manufacturing and product lifecycle management in industry 4.0: a survey. Renew. Sustain. Energy Rev. **132**, 110112 (2020). https://doi.org/10.1016/j.rser.2020.110112
40. Nuttah, M.M., Roma, P., Lo Nigro, G., Perrone, G.: Understanding blockchain applications in Industry 4.0: From information technology to manufacturing and operations management. J. Ind. Inf. Integr. **33**, 100456 (2023). https://doi.org/10.1016/j.jii.2023.100456
41. Gimenez-Aguilar, M., Maria, J., de Fuentes, L., Gonzalez-Manzano, D.A.: Achieving cybersecurity in blockchain-based systems: a survey. Future Gener. Comput. Syst. **124**, 91–118 (2021). https://doi.org/10.1016/j.future.2021.05.007
42. Hasanova, H., Baek, U.-J., Shin, M.-G., Cho, K., Kim, M.-S.: A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. Int. J. Netw. Manag. **29**(2), e2060 (2019). https://doi.org/10.1002/nem.2060
43. Raimundo, R.J., Rosário, A.T.: Cybersecurity in the internet of things in industrial management. Appl. Sci. **12**(3), 1598 (2022). https://doi.org/10.3390/app12031598
44. IEEE. "IEEE Standard for Architectural Framework and Technical Requirements for Smart Display Systems." IEEE Emerging Technology Standards Committee. https://standards.ieee.org/ieee/2868/10217/ (accessed Oct 5, 2023).
45. Armenta, A.: "Components of the Industrial Internet of Things." Control Automation. https://control.com/technical-articles/components-of-the-industrial-internet-of-things/ (accessed Oct 4, 2023).
46. BasuMallick, C.: What Is IIoT (Industrial Internet of Things)? Definition, Architecture, Benefits, and Examples." https://www.spiceworks.com/tech/iot/articles/what-is-iiot/ (accessed Oct 3, 2023).
47. TrendMicro. Threats and consequences. https://www.trendmicro.com/vinfo/us/security/news/Internet-of-things/threats-and-consequences-a-security-analysis-of-smart-manufacturing-systems (accessed Oct 20, 2023).
48. N. I. A. P. Ltd. "Connecting the IIoT." Process Technology. https://www.processonline.com.au/content/software-it/article/connecting-the-iiot-947158535 (accessed Oct 15, 2023).
49. Mantravadi, S., Schnyder, R., Møller, C., Brunoe, T.D.: Securing IT/OT links for low power IIoT devices: design considerations for industry 4.0. IEEE Access **8**, 200305–200321 (2020). https://doi.org/10.1109/ACCESS.2020.3035963
50. Alladi, T., Chamola, V., Zeadally, S.: Industrial control systems: cyberattack trends and countermeasures. Comput. Commun. **155**, 1–8 (2020). https://doi.org/10.1016/j.comcom.2020.03.007
51. TREND. "Why Do Attackers target industrial control systems?" https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/why-do-attackers-target-industrial-control-systems (accessed Oct 5, 2023).
52. Tariq, N., Asim, M., Khan, F.A.: Securing SCADA-based critical infrastructures: challenges and open issues. Procedia Comput. Sci. **155**, 612–617 (2019). https://doi.org/10.1016/j.procs.2019.08.086
53. Hammad, M., Badshah, A., Abbas, G., Alasmary, H., Waqas, M., Khan, W.A.: A Provable secure and efficient authentication framework for smart manufacturing industry. IEEE Access **11**, 67626–67639 (2023). https://doi.org/10.1109/ACCESS.2023.3290913
54. Tanveer, M., Badshah, A., Khan, A.U., Alasmary, H., Chaudhry, S.A.: CMAF-IIoT: Chaotic map-based authentication framework for Industrial internet of things. Internet Things **23**, 100902 (2023). https://doi.org/10.1016/j.iot.2023.100902
55. Tanveer, M., Alkhayyat, A., Khan, A.U., Kumar, N., Alharbi, A.G.: REAP-IIoT: Resource-efficient authentication protocol for the industrial internet of things. IEEE Internet Things J. **9**(23), 24453–24465 (2022). https://doi.org/10.1109/JIOT.2022.3188711
56. Wang, K., Sun, K., Dong, J., Sha, L., Xiao, F.: AP-CDE: Cost-efficient authentication protocol for cross-domain data exchange in IIoT. IEEE Syst. J. **17**(3), 3882–3893 (2023). https://doi.org/10.1109/JSYST.2023.3269046

57. Srinivas, J., Das, A.K., Wazid, M., Kumar, N.: Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial internet of things. IEEE Trans. Dependable Secure Comput. **17**(6), 1133–1146 (2020). https://doi.org/10.1109/TDSC.2018.2857811
58. Das, A.K., Wazid, M., Kumar, N., Vasilakos, A.V., Rodrigues, J.J.P.C.: Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment. IEEE Internet Things J. **5**(6), 4900–4913 (2018). https://doi.org/10.1109/JIOT.2018.2877690
59. Patel, C., Bashir, A.K., AlZubi, A.A., Jhaveri, R.: EBAKE-SE: A novel ECC-based authenticated key exchange between industrial IoT devices using secure element. Digit. Commun. Netw. **9**(2), 358–366 (2023). https://doi.org/10.1016/j.dcan.2022.11.001
60. Xu, D., Yu, K., Ritcey, J.A.: Cross-layer device authentication with quantum encryption for 5g enabled IIoT in industry 4.0. IEEE Trans. Industr. Inf. **18**(9), 6368–6378 (2022). https://doi.org/10.1109/TII.2021.3130163
61. Cui, J., Wang, F., Zhang, Q., Xu, Y., Zhong, H.: Anonymous message authentication scheme for semitrusted edge-enabled IIoT. IEEE Trans. Industr. Electron. **68**(12), 12921–12929 (2021). https://doi.org/10.1109/TIE.2020.3039227
62. El-Zawawy, M.A., Kaliyar, P., Conti, M., Katsikas, S.: Honey-list based authentication protocol for industrial IoT swarms. Comput. Commun. **211**, 239–253 (2023). https://doi.org/10.1016/j.comcom.2023.09.012
63. Koprov, P., Gadhwala, S., Walimbe, A., Fang, X., Starly, B.: Systems and methods for authenticating manufacturing Machines through an unobservable fingerprinting system. Manuf. Lett. **35**, 1009–1018 (2023). https://doi.org/10.1016/j.mfglet.2023.08.051
64. Zhang, Y., Li, B., Wu, J., Liu, B., Chen, R., Chang, J.: Efficient and Privacy-preserving blockchain-based multifactor device authentication protocol for cross-domain IIoT. IEEE Internet Things J. **9**(22), 22501–22515 (2022). https://doi.org/10.1109/JIOT.2022.3176192
65. Shen, M., et al.: Blockchain-assisted secure device authentication for cross-domain industrial IoT. IEEE J. Sel. Areas Commun. **38**(5), 942–954 (2020). https://doi.org/10.1109/JSAC.2020.2980916
66. Li, D., et al.: Blockchain-based authentication for IIoT devices with PUF. J. Syst. Archit. **130**, 102638 (2022). https://doi.org/10.1016/j.sysarc.2022.102638
67. Sharma, P.C., Mahmood, M.R., Raja, H., Yadav, N.S., Gupta, B.B., Arya, V.: Secure authentication and privacy-preserving blockchain for industrial internet of things. Comput. Electr. Eng. **108**, 108703 (2023). https://doi.org/10.1016/j.compeleceng.2023.108703
68. Imperva. Role-Based Access Control (RBAC). https://www.imperva.com/learn/data-security/role-based-access-control-rbac/ (accessed Oct 20, 2023).
69. Security, C.: Rule-based Access Control." https://www.caldersecurity.co.uk/rule-based-access-control/ (accessed Oct 2023, 2023).
70. Labs, N.: "Attribute-Based Access Control (ABAC)." https://www.nextlabs.com/products/technology/abac/ (accessed Oct 20, 2023).
71. Saha, R., et al.: DHACS: smart contract-based decentralized hybrid access control for industrial internet-of-things. IEEE Trans. Industr. Inf. **18**(5), 3452–3461 (2022). https://doi.org/10.1109/TII.2021.3108676
72. Cui, J., et al.: An anonymous and outsourcing-supported multi-authority access control scheme with revocation for edge-enabled IIoT system. IEEE Syst. J. **16**(4), 6569–6580 (2022). https://doi.org/10.1109/JSYST.2022.3189219
73. Wang, W., Huang, H., Yin, Z., Gadekallu, T.R., Alazab, M., Chunhua, S.: Smart contract token-based privacy-preserving access control system for industrial Internet of Things. Digit. Commun. Netw. **9**(2), 337–346 (2023). https://doi.org/10.1016/j.dcan.2022.10.005
74. Bera, B., Chattaraj, D., Das, A.K.: Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment. Comput. Commun. **153**, 229–249 (2020). https://doi.org/10.1016/j.comcom.2020.02.011
75. Nakamura, Y., Zhang, Y., Sasabe, M., Kasahara, S.: Exploiting smart contracts for capability-based access control in the internet of things. Sensors **20**(6), 1793 (2020). https://doi.org/10.3390/s20061793
76. Liu, H., Han, D., Li, D.: Fabric-IoT: A blockchain-based access control system in IoT. IEEE Access **8**, 18207–18218 (2020). https://doi.org/10.1109/ACCESS.2020.2968492
77. Ding, S., Cao, J., Li, C., Fan, K., Li, H.: A novel attribute-based access control scheme using blockchain for IoT. IEEE Access **7**, 38431–38441 (2019). https://doi.org/10.1109/ACCESS.2019.2905846
78. Nasiraee, H., Ashouri-Talouki, M.: Anonymous decentralized attribute-based access control for cloud-assisted IoT. Future Gener. Comput. Syst. **110**, 45–56 (2020). https://doi.org/10.1016/j.future.2020.04.011
79. Figueroa-Lorenzo, S., Añorga, J., Arrizabalaga, S.: Methodological performance analysis applied to a novel IIoT access control system based on permissioned blockchain. Inf. Process. & Manag. **58**(4), 102558 (2021). https://doi.org/10.1016/j.ipm.2021.102558
80. Salim, M.M., El Azzaoui, A., Deng, X., Park, J.H.: FL-CTIF: A federated learning based CTI framework based on information fusion for secure IIoT. Inf. Fusion **102**, 102074 (2024). https://doi.org/10.1016/j.inffus.2023.102074
81. Halder, S., Newe, T.: Enabling secure time-series data sharing via homomorphic encryption in cloud-assisted IIoT. Future Gener. Comput. Syst. **133**, 351–363 (2022). https://doi.org/10.1016/j.future.2022.03.032
82. Gilles, O., Gracia Pérez, D., Brameret, P.-A., Lacroix, V.: Securing IIoT communications using OPC UA PubSub and trusted platform modules. J. Syst. Archit. **134**, 102797 (2023). https://doi.org/10.1016/j.sysarc.2022.102797
83. Lin, H., Hu, J., Wang, X., Alhamid, M.F., Piran, M.J.: Toward secure data fusion in industrial IoT Using transfer learning. IEEE Trans. Industr. Inf. **17**(10), 7114–7122 (2021). https://doi.org/10.1109/TII.2020.3038780
84. Umran, S.M., SongFeng, L., Abduljabbar, Z.A., Nyangaresi, V.O.: Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet Things **24**, 100969 (2023). https://doi.org/10.1016/j.iot.2023.100969
85. Lu, J., Shen, J., Vijayakumar, P., Gupta, B.B.: Blockchain-based secure data storage protocol for sensors in the industrial internet of things. IEEE Trans. Industr. Inf. **18**(8), 5422–5431 (2022). https://doi.org/10.1109/TII.2021.3112601
86. Jiang, Y., Zhong, Y., Ge, X.: IIoT data sharing based on blockchain: a multileader multifollower stackelberg game approach. IEEE Internet Things J. **9**(6), 4396–4410 (2022). https://doi.org/10.1109/JIOT.2021.3103855
87. Jiang, Y., Zhong, Y., Ge, X.: Smart contract-based data commodity transactions for industrial internet of things. IEEE Access **7**, 180856–180866 (2019). https://doi.org/10.1109/ACCESS.2019.2959771
88. Yu, K., Tan, L., Aloqaily, M., Yang, H., Jararweh, Y.: Blockchain-enhanced data sharing with traceable and direct revocation in IIoT. IEEE Trans. Industr. Inf. **17**(11), 7669–7678 (2021). https://doi.org/10.1109/TII.2021.3049141
89. Kumari, A., Tanwar, S., Tyagi, S., Kumar, N.: Blockchain-based massive data dissemination handling in IIoT environment. IEEE

Network **35**(1), 318–325 (2021). https://doi.org/10.1109/MNET.011.2000355
90. Yu, X., Xie, Y., Xu, Q., Xu, Z., and Xiong, R.: Secure data sharing for cross-domain industrial iot based on consortium blockchain, In: 2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD), 24–26, pp. 1508–1513, (2023) https://doi.org/10.1109/CSCWD57460.2023.10152584.
91. Ma, R., Zhang, L., Wu, Q., Mu, Y., Rezaeibagha, F.: BE-TRDSS: Blockchain-enabled secure and efficient traceable-revocable data-sharing scheme in industrial internet of things. IEEE Trans. Industr. Inf. **19**(11), 10821–10830 (2023). https://doi.org/10.1109/TII.2023.3241618
92. Xu, H., He, Q., Li, X., Jiang, B., Qin, K.: BDSS-FA: a blockchain-based data security sharing platform with fine-grained access control. IEEE Access **8**, 87552–87561 (2020). https://doi.org/10.1109/ACCESS.2020.2992649
93. Abdullahi, S.M., Sun, S., Wang, B., Wei, N., Wang, H.: Biometric template attacks and recent protection mechanisms: a survey. Inf. Fusion **103**, 102144 (2024). https://doi.org/10.1016/j.inffus.2023.102144
94. Abdullahi, S.M., Lv, K., Sun, S., Wang, H.: Cancelable fingerprint template construction using vector permutation and shift-ordering. IEEE Trans. Dependable Secure Comput. **20**(5), 3828–3844 (2023). https://doi.org/10.1109/TDSC.2022.3213704
95. Abdullahi, S.M., Wang, H., Li, T.: Fractal coding-based robust and alignment-free fingerprint image hashing. IEEE Trans. Inf. Forensics Secur. **15**, 2587–2601 (2020). https://doi.org/10.1109/TIFS.2020.2971142
96. Abdullahi, S.M., Sun, S., Wang, Y., Yang, P., Wang, H., Wang, B.: A hybrid BTP approach with filtered BCH codes for improved performance and security. J. Inf. Secur. Appl. **71**, 103355 (2022). https://doi.org/10.1016/j.jisa.2022.103355
97. Oliveira, G.W.D., Nogueira, M., Luiz, A., dos Santos, D., Batista, M.: Intelligent VNF placement to mitigate DDoS attacks on industrial IoT. IEEE Trans. Netw. Service Manag. **20**(2), 1319–1331 (2023). https://doi.org/10.1109/TNSM.2023.3274364
98. Siriweera, A., Naruse, K.: QoS-aware federated crosschain-based model-driven reference architecture for IIoT sensor networks in distributed manufacturing. IEEE Sens. J. **23**(23), 29630–29644 (2023). https://doi.org/10.1109/JSEN.2023.3325342
99. Atutxa, A., Astorga, J., Barcelo, M., Urbieta, A., Jacob, E.: Improving efficiency and security of IIoT communications using in-network validation of server certificate. Comput. Industry **144**, 103802 (2023). https://doi.org/10.1016/j.compind.2022.103802
100. Khan, I.A., Keshk, M., Pi, D., Khan, N., Hussain, Y., Soliman, H.: Enhancing IIoT networks protection: A robust security model for attack detection in internet industrial control systems. Ad Hoc Netw. **134**, 102930 (2022). https://doi.org/10.1016/j.adhoc.2022.102930
101. Deshpande, S., Padalkar, S., Anand, S.: IIoT based framework for data communication and prediction using augmented reality for legacy machine artifacts. Manuf. Lett. **35**, 1043–1051 (2023). https://doi.org/10.1016/j.mfglet.2023.08.058
102. Illy, P., Kaddoum, G.: A collaborative DNN-based low-latency IDPS for mission-critical smart factory networks. IEEE Access **11**, 96317–96329 (2023). https://doi.org/10.1109/ACCESS.2023.3311822
103. Chaudhary, R., Aujla, G.S., Garg, S., Kumar, N., Rodrigues, J.J.P.C.: SDN-enabled multi-attribute-based secure communication for smart grid in IIoT environment. IEEE Trans. Industr. Inf. **14**(6), 2629–2640 (2018). https://doi.org/10.1109/TII.2018.2789442
104. Pokhrel, S.R., Garg, S.: Multipath communication with deep Q-network for industry 4.0 automation and orchestration. IEEE Trans. Industr. Inf. **17**(4), 2852–2859 (2021). https://doi.org/10.1109/TII.2020.3000502
105. Zhu, M., Chang, L., Wang, N., You, I.: A smart collaborative routing protocol for delay sensitive applications in industrial IoT. IEEE Access **8**, 20413–20427 (2020). https://doi.org/10.1109/ACCESS.2019.2963723
106. Jagtap, S.S., Kotecha, S.V.V.S.K., Subramaniyaswamy, V.S.: Securing industrial control systems from cyber-attacks: a stacked neural-network-based approach. IEEE Consum. Electron. Mag. **13**(1), 30–38 (2024). https://doi.org/10.1109/MCE.2022.3168997
107. Yazdinejad, A., Dehghantanha, A., Parizi, R.M., Hammoudeh, M., Karimipour, H., Srivastava, G.: Block hunter: federated learning for cyber threat hunting in blockchain-based IIoT networks. IEEE Trans. Industr. Inf. **18**(11), 8356–8366 (2022). https://doi.org/10.1109/TII.2022.3168011
108. Yin, H., Zhang, W., Deng, H., Qin, Z., Li, K.: An attribute-based searchable encryption scheme for cloud-assisted IIoT. IEEE Internet Things J. **10**(12), 11014–11023 (2023). https://doi.org/10.1109/JIOT.2023.3242964
109. Zhang, X., Xu, C., Wang, H., Zhang, Y., Wang, S.: FS-PEKS: Lattice-based forward secure public-key encryption with keyword search for cloud-assisted industrial internet of things. IEEE Trans. Dependable Secure Comput. **18**(3), 1019–1032 (2021). https://doi.org/10.1109/TDSC.2019.2914117
110. Lu, Y., Li, J., Zhang, Y.: Privacy-preserving and pairing-free multirecipient certificateless encryption with keyword search for cloud-assisted IIoT. IEEE Internet Things J. **7**(4), 2553–2562 (2020). https://doi.org/10.1109/JIOT.2019.2943379
111. Anichur Rahman, Md., Islam, J., Band, S.S., Muhammad, G., Hasan, K., Tiwari, P.: Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT. Digit. Commun. Netw. **9**(2), 411–421 (2023). https://doi.org/10.1016/j.dcan.2022.11.003
112. Li, Q., Yue, Y., Wang, Z.: Deep robust cramer shoup delay optimized fully homomorphic For IIOT secured transmission in cloud computing. Comput. Commun. **161**, 10–18 (2020). https://doi.org/10.1016/j.comcom.2020.06.017
113. Humayun, M., Jhanjhi, N., Alruwaili, M., Amalathas, S.S., Balasubramanian, V., Selvaraj, B.: Privacy protection and energy optimization for 5G-aided industrial internet of things. IEEE Access **8**, 183665–183677 (2020). https://doi.org/10.1109/ACCESS.2020.3028764
114. Xiaoxiao, X., Han, M., Nagarajan, S.M., Anandhan, P.: Industrial internet of things for smart manufacturing applications using hierarchical trustful resource assignment. Comput. Commun. **160**, 423–430 (2020). https://doi.org/10.1016/j.comcom.2020.06.004
115. Chen, Y., et al.: Cryptanalysis and improvement of DeepPAR: privacy-preserving and asynchronous deep learning for industrial IoT. IEEE Internet Things J. **9**(21), 21958–21970 (2022). https://doi.org/10.1109/JIOT.2022.3181665
116. Han, Q., Yang, S., Ren, X., Zhao, P., Zhao, C., Wang, Y.: PCFed: privacy-enhanced and communication-efficient federated learning for industrial IoTs. IEEE Trans. Industr. Inf. **18**(9), 6181–6191 (2022). https://doi.org/10.1109/TII.2022.3161673
117. Bugshan, N., Khalil, I., Rahman, M.S., Atiquzzaman, M., Yi, X., Badsha, S.: Toward trustworthy and privacy-preserving federated deep learning service framework for industrial internet of things. IEEE Trans. Industr. Inf. **19**(2), 1535–1547 (2023). https://doi.org/10.1109/TII.2022.3209200
118. Li, S., Ngai, E., Voigt, T.: Byzantine-robust aggregation in federated learning empowered industrial IoT. IEEE Trans. Industr. Inf. **19**(2), 1165–1175 (2023). https://doi.org/10.1109/TII.2021.3128164
119. Wang, X., et al.: QoS and privacy-aware routing for 5G-enabled industrial internet of things: a federated reinforcement learning approach. IEEE Trans. Industr. Inf. **18**(6), 4189–4197 (2022). https://doi.org/10.1109/TII.2021.3124848

120. Wang, X., et al.: Toward accurate anomaly detection in industrial internet of things using hierarchical federated learning. IEEE Internet Things J. **9**(10), 7110–7119 (2022). https://doi.org/10.1109/JIOT.2021.3074382
121. Zheng, C., Liu, S., Huang, Y., Zhang, W., Yang, L.: Unsupervised recurrent federated learning for edge popularity prediction in privacy-preserving mobile-edge computing networks. IEEE Internet Things J. **9**(23), 24328–24345 (2022). https://doi.org/10.1109/JIOT.2022.3189055
122. Pandey, A.K., Saxena, R., Awasthi, A., Sunil, M.P.: Privacy preserved data sharing using blockchain and support vector machine for industrial IOT applications. Meas. Sens. **29**, 100891 (2023). https://doi.org/10.1016/j.measen.2023.100891
123. Bao, Z., He, D., Khan, M.K., Luo, M., Xie, Q.: PBidm: privacy-preserving blockchain-based identity management system for industrial internet of things. IEEE Trans. Industr. Inf. **19**(2), 1524–1534 (2023). https://doi.org/10.1109/TII.2022.3206798
124. Park, K., Lee, J., Das, A.K., Park, Y.: BPPS:blockchain-enabled privacy-preserving scheme for demand-response management in smart grid environments. IEEE Trans. Dependable Secure Comput. **20**(2), 1719–1729 (2023). https://doi.org/10.1109/TDSC.2022.3163138
125. Gao, B., Yan, H., and Tian, R.: A Privacy-aware cross-domain device authentication scheme for IIoT based on blockchain," In: *2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys)*, pp. 561-570, (2021) https://doi.org/10.1109/HPCC-DSS-SmartCity-DependSys53884.2021.00097
126. Singh, S.K., Yang, L.T., Park, J.H.: FusionFedBlock: fusion of blockchain and federated learning to preserve privacy in industry 5.0. Inf. Fusion **90**, 233–240 (2023). https://doi.org/10.1016/j.inffus.2022.09.027
127. Duy, P.T., Quyen, N.H., Khoa, N.H., Tran, T.-D., Pham, V.-H.: FedChain-hunter: a reliable and privacy-preserving aggregation for federated threat hunting framework in SDN-based IIoT. Internet Things **24**, 100966 (2023). https://doi.org/10.1016/j.iot.2023.100966
128. Zhou, W., Jia, Y., Peng, A., Zhang, Y., Liu, P.: The effect of iot new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. IEEE Internet Things J. **6**(2), 1606–1616 (2019). https://doi.org/10.1109/JIOT.2018.2847733
129. DigitalOcean. Prometheus: From metrics to insight. https://prometheus.io/ (accessed August 24, 2023).
130. GrafanaLabs. Grafana. https://grafana.com/ (accessed Aug 24, 2023).
131. Watts, S.: Network Configuration Today: The Ultimate Guide. https://www.splunk.com/en_us/blog/learn/network-configuration.html (accessed September 15, 2023).
132. GDPR. E., General data protection regulation. https://gdpr-info.eu/ (accessed Oct 29, 2023).
133. GDPR, Regulations, EU GDPR, 2016. Accessed: Oct 29, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1473816357502&from=en
134. CCPA. California Consumer Privacy Act. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (accessed Oct 29, 2023).
135. IIC, Industrial IoT Consortium, In: Data Protection best practices: an industrial internet consortium white paper, (2019). Accessed: Oct 2023. [Online]. Available: https://www.iiconsortium.org/pdf/Data_Protection_Best_Practices_Whitepaper_2019-07-22.pdf
136. Ottolini,D., Zyrianoff, I., and Kamienski, C., Interoperability and scalability trade-offs in open IoT platforms," In: *2022 IEEE* 19th Annual Consumer Communications & Networking Conference (CCNC), 8–11, pp. 1–6, (2022) https://doi.org/10.1109/CCNC49033.2022.9700622.
137. Portelli, K., and Anagnostopoulos, C.: Leveraging edge computing through collaborative machine learning, In: 2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), 21–23, pp. 164–169, (2017) https://doi.org/10.1109/FiCloudW.2017.72.
138. Díaz, M., Martín, C., and Rubio, B.: CoAP: An internet of things and cloud computing integration based on the lambda architecture and CoAP," Cham: Springer International Publishing, in Collaborative Computing: Networking, Applications, and Worksharing, pp. 195–206. (2016)
139. Wang, S. *et al.*, When Edge meets learning: adaptive control for resource-constrained distributed machine learning, In: IEEE INFOCOM 2018—IEEE Conference on Computer Communications, 16–19, pp. 63–71, (2018) https://doi.org/10.1109/INFOCOM.2018.8486403.
140. Portal, G., Matos, E.D., Hessel, F.: An Edge Decentralized Security Architecture for Industrial IoT Applications, In: 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), 2–16, pp. 1–6, (2020) https://doi.org/10.1109/WF-IoT48130.2020.9221176.
141. Zheng, X., Yang, S., Wang, X.: A reliable and decentralized trust management model for fog computing in industrial IoT, In: NOMS 2023–2023 IEEE/IFIP Network Operations and Management Symposium, 8–12, pp. 1–6, (2023) https://doi.org/10.1109/NOMS56928.2023.10154305.
142. Breiki, H.A., Qassem, L.A., Salah, K., Rehman, M.H.U., Sevtinovic, D.: Decentralized access control for IoT Data using blockchain and trusted oracles, In: 2019 IEEE International Conference on Industrial Internet (ICII), 11–12, pp. 248–257, (2019) https://doi.org/10.1109/ICII.2019.00051.
143. Qiu, W., Ai, W., Chen, H., Feng, Q., Tang, G.: Decentralized federated learning for industrial IoT with deep echo state networks. IEEE Trans. Industr. Inf. **19**(4), 5849–5857 (2023). https://doi.org/10.1109/TII.2022.3194627
144. Ahmed, M., Jaidka, S., Sarkar, N.I.: Security in Decentralised Computing, IoT and Industrial IoT. In: Butun, I. (ed.) Industrial IoT: Challenges, Design Principles, Applications, and Security, pp. 191–211. Springer, Cham (2020)