Received 23 December 2023; accepted 15 January 2024. Date of publication 19 January 2024; date of current version 9 February 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.3356076

Communications Security in Industry X: A Survey

IJAZ AHMAD[1] (Senior Member, IEEE), FELIPE RODRIGUEZ[2], TANESH KUMAR[3] (Member, IEEE), JANI SUOMALAINEN[1], SENTHIL KUMAR JAGATHEESAPERUMAL[4], STEFAN WALTER[1], MUHAMMAD ZEESHAN ASGHAR[5], GAOLEI LI[6] (Member, IEEE), NIKOLAOS PAPAKONSTANTINOU[1], MIKA YLIANTTILA[2] (Senior Member, IEEE), JYRKI HUUSKO[1], THILO SAUTER[7,8] (Fellow, IEEE), AND ERKKI HARJULA[3] (Member, IEEE)

[1]VTT Technical Research Centre of Finland, 02150 Espoo, Finland

[2]Nokia, Espoo, Finland

[3]Centre of Wireless Communications, University of Oulu, 90570 Oulu, Finland

[4]Department of Electronics and Communication Engineering, Mepco Schlenk Engineering College, Sivakasi 626005, India

[5]Enfuce Financial Services, Espoo, Finland

[6]Institute of Cyber Security, Shanghai Jiao Tong University, Shanghai 200240, China

[7]TU Wien, Vienna, Austria,

[8]University of Continuing Education Krems, Wiener Neustadt, Austria

CORRESPONDING AUTHOR: I. AHMAD (e-mail: ijaz.ahmad@vtt.fi)

This work was supported in part by Business Finland through the SUNSET-6G and the AI-NET-ANTILLAS Projects; in part by the Academy of Finland under 6Genesis Flagship under Grant 346208; and in part by SafeSecLab, a joint Project of TU Wien and TUV Austria.

ABSTRACT Industry 4.0 is moving towards deployment using 5G as one of the main underlying communication infrastructures. Thus, the vision of the Industry of the future is getting more attention in research. Industry X (InX) is a significant thrust beyond the state-of-the-art of current Industry 4.0, towards a mix of cyber and physical systems through novel technological developments. In this survey, we define InX as the combination of Industry 4.0 and 5.0 paradigms. Most of the novel technologies, such as cyber-physical systems, industrial Internet of things, machine learning, advances in cloud computing, such as edge and fog computing, and blockchain, to name a few, are converged through advanced communication networks. Since communication networks are usually targeted for security attacks, these new technologies upon which InX relies must be secured to avoid security vulnerabilities propagating into InX and its components. Therefore, in this article, we break down the security concerns of the converged InX-communication networks into the core technologies that tie these, once considered distinct, fields together. The security challenges of each technology are highlighted and potential solutions are discussed. The existing vulnerabilities or research gaps are brought forth to stir further research in this direction. New emerging visions in the context of InX are provided towards the end of the article to provoke further curiosity of researchers.

INDEX TERMS Industry 4.0, industrial systems, communications networks, security, cyber-physical systems, IIoT, IIoT security, risk management, industrial control system, 5G.

I. INTRODUCTION

MOVING through the ladder of the industrial revolution on its logical path [1], the industry of the future or Industry X (InX) couples the digital and physical world through novel scientific and technological transformations, beyond Industry 4.0. Industry 4.0 [2], is the present big industrial transformation after mechanization, electrification, and information were introduced, and it is considered a key step in the advancement of the industry to its state-of-the-art [3]. Industry 5.0 is often seen as the extension of Industry 4.0 (focusing on data-driven applications and connectivity) towards the adoption of advanced artificial intelligence (AI) technologies for industrial automation and human-robot collaboration [4]. The European Union (EU) commission

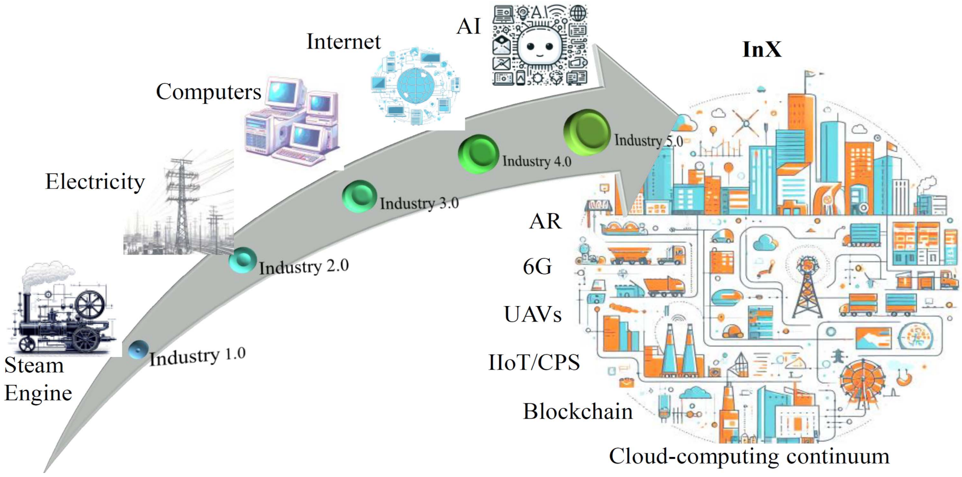

FIGURE 1. Continuum from Industry 1.0 to Industry 5.0, and then converging to InX.

envisions Industry 5.0 as an extension that will focus on and be an enabler for advanced R&D, investment for up- and re-skilling of workers, circular economy, and human-centric adoption of digital technologies and AI [5]. InX is a combination of technology paradigms in Industry 4.0 and 5.0, as well as drivers and processes enabling the continuous evolution of industry beyond Industry 5.0.

The foundations of Industry 4.0, i.e., connectivity of industrial systems, processes, and services through novel communication networks, have become pivotal to the success of InX [6]. The fifth-generation wireless networking, known as 5G, facilitates the envisioned humongous growth of the Industrial Internet of Things (IIoT), and cyber-physical systems (CPS), providing extremely low latency connectivity for critical functions of InX. However, advanced communications networks have their security challenges and require novel solutions for mitigating these challenges [7], [8]. The key technologies of Industry 4.0 include mobile Internet, IoT, CPS, cloud computing, big data, and advanced analytics techniques [3]. From the communications perspective, each of these has its security weaknesses and vulnerabilities and when combined into an ecosystem, the emerging complexity due to mixed criticality [9] can further exacerbate the challenges. Therefore, a thorough analysis of the security of the underlying communication systems and technologies is necessary from many perspectives, yet the main one is the improvement of the overall resilience of critical InX applications enabling their uninterrupted role in our societies.

The security weaknesses in the enabling technologies of InX, which can be used by malicious internal and external actors, must be properly studied. For instance, weaknesses of most IoT devices in using proper encryption techniques must also be brought forth to avoid sending or redirecting sensitive information through such devices. Similarly, if physical access to CPS systems cannot be restricted, proper security mechanisms must be in place to avoid tampering even with physical access. Furthermore, communication networks, such as 5G, have loopholes in terms of security as clearly elaborated and outlined in [7], [10]. InX relies on such communication networks to connect critical infrastructure and its elements, such as IIoT and CPS [11]. The EU Commission recognizes these emerging challenges and places resilience as one of the three main pillars of Industry 5.0. Therefore, security concerns related to the enabling technologies of InX, such as 5G, CPS, IIoT, etc., must be considered at all levels and resolved to avoid possible cascading effects due to the reliance of technologies on each other.

A. ROADMAP TO INX: MOTIVATION

The industrial revolutions have transformed the quality of life of most of the world by changing the means of production from human-intensive to machine-intensive. Scientific and technological innovations brought the revolutions that changed the ways of working, living, using resources, and human experiences. The first industrial revolution (Industry 1.0) (1760-1840) was mainly characterized by the mechanization of production and steam power. The second industrial revolution (Industry 2.0) (1870-1920) was mainly driven by electricity and the development of the internal combustion engine. The third industrial revolution (Industry 3.0) (1960-2000) was characterized by the development of electronics, computers, and telecommunications. The fourth industrial revolution (Industry 4.0) (2000-2025) is attributed to the development of Internet technologies, whereas the fifth industrial revolution (Industry 5.0) (beyond 2025) revolves around the role of AI. Industry X, the term used in this paper, engulfs Industry 5.0 and beyond and is described in the rest of this subsection. These revolutions are also depicted in Fig. 1. It is important to note that there are differences in definitions and variations in the time spans of the revolutions. However, the aim is to provide a brief generic background for the rest of the study of this paper.

Industry 4.0 has become a center of attraction in developed countries and a strong strategic or even political goal in the first place [12]. Even though it is considered a fundamental paradigm shift in industrial production with great expectations for innovation, the concept of Industry 4.0 is only loosely defined and heavily linked to the technological developments in the last decade [13]. Considered the driving force behind innovation in many fields and dimensions of social development, Industry 4.0 is not a singleton technological development, but rather an ecosystem that provides an umbrella of distinct technological developments under the guise of industry of the future [14].

The main features of Industry 4.0 include i) horizontal integration through value networks to facilitate collaboration among corporate sectors, ii) vertical integration of hierarchical subsystems in a factory to create a flexible and re-configurable manufacturing system, and (iii) end-to-end engineering integration across entire value chains to support customization of products [2], [11], [15]. These features indicate a strong need for the integration of various systems and services that may comprise different combinations of the above stages and can be in different geographical locations. Therefore, the security of the communication systems that facilitate integrating the systems of Industry 4.0 is of paramount importance due to the critical nature of the infrastructure.

The basic design principles of Industry 4.0 are i) interconnection, ii) information transparency, iii) decentralized decisions, and iv) technical assistance [16]. Communication is a core requirement to implement these principles. Therefore, beyond traditional industrial communication, the major enabler of Industry 4.0 has been the introduction of Internet technologies to achieve the required massive interconnection on and across all levels [6]. This includes modern cloud concepts as well as the IoT and goes far beyond individual remote connections to production facilities that have been discussed already 25 years ago. On the downside, the strong reliance on Internet technologies and the increasing use of IT devices on the factory floor has also brought cyber-threats closer to the industrial environments where they have an impact on the safety and stability of production systems [17].

The European Commission formally introduced the term “Fifth Industrial Revolution (Industry 5.0)” in 2021 through the Directorate-General for Research and Innovation [18]. The main aim as discussed in [18] was to initiate a wider debate on shaping Industry 5.0 in the European context. Industry 5.0 revolves around three main drivers, i.e., i) Sustainability, ii) Resilience, and iii) Human-centricity, as defined by the European Commission [18]. Even though the roots of Industry 5.0 are in the concepts of Industry 4.0, the focus of Industry 5.0 remains on long-term service to humanity within our planetary boundaries, highlights the European Commission. The concepts of Industry 5.0 and Society 5.0, a term coined by the Japanese, are related in the sense that Society 5.0 represents a society after the dominance of “information” and ripe with the use of IT technologies, IoT, AI, robots, and AR, all serving humanity in everyday life and every sphere including industries [18]. Even though Industry 5.0 is human-centric, its emphasis on advanced digitization, big data, and AI in the digital sphere will meet new and emerging requirements of the future industrial landscape, such as InX.

Being one of the three main visions, resilience is the key pillar to develop a higher degree of robustness in industrial production to work normally during disruptions, and even provide support to critical infrastructure during times of crisis. Even though resilience can be defined according to a specific context, generally resilience is *“the capacity of a system to absorb disturbances while responding to an ongoing change so that the system can sustain its function, structure, and output levels”* [19], whereas, technological resilience allows industries to adopt to and respond to crisis [20]. Industry 5.0 must have resilient strategic value chains, adaptable production capacity, as well as enough flexibility in the business processes. Furthermore, resilience enables the industry to cope flexibly with disruptive changes, and vulnerabilities on many levels including the factory floor, supply networks, and industrial systems. However, the general trend in innovation focuses on efficiency, whereas resilience is mostly overlooked.

Since the main differentiating pillars of InX from the earlier industrial revolutions are emerging technologies, cybersecurity becomes the main pillar to make InX as resilient as required. Therefore, the security of the most important enabling technologies needs a thorough investigation. Since communication technologies connect the vital components of the industrial ecosystem, the security of communication technologies comes to the forefront for securing the overall ecosystem. It is important to note that the main driving force for evolution from Industry 4.0 to Industry 5.0 is remote production with distributed value chain [21] that requires fool-proof security of enabling connectivity technologies. Therefore, in this article, we focus on all technological enablers of InX that are used either as communication media or require digital communication for its very functionality. Fig. 2 highlights the scope of our paper, where each underlying enabling technology converges for enabling InX. We are looking at the security aspects of the most relevant technological enablers, as well as the impacts arising from their integration into Industry 4.0 and 5.0 concepts. Furthermore, we are looking at the security enablers and challenges of future technologies adopted by InX.

This work is motivated by the increasing cyber security challenges related to the technological enablers of InX. As depicted in Fig. 2, many technologies will converge in InX, and each enabling technology, such as 5G, IIoT, AI, and AR, to name a few, has its security challenges. With its integration into InX, the overall security threat landscape will hugely increase. For example, the security threats in 5G as explained in [22] can expose production lines to security threats if insecure 5G base stations provide the connectivity between different assembly lines. Similarly, AI has many security challenges as explained in [23], which can cause serious harm in several operations, such as during monitoring and maintenance, in the InX ecosystem.

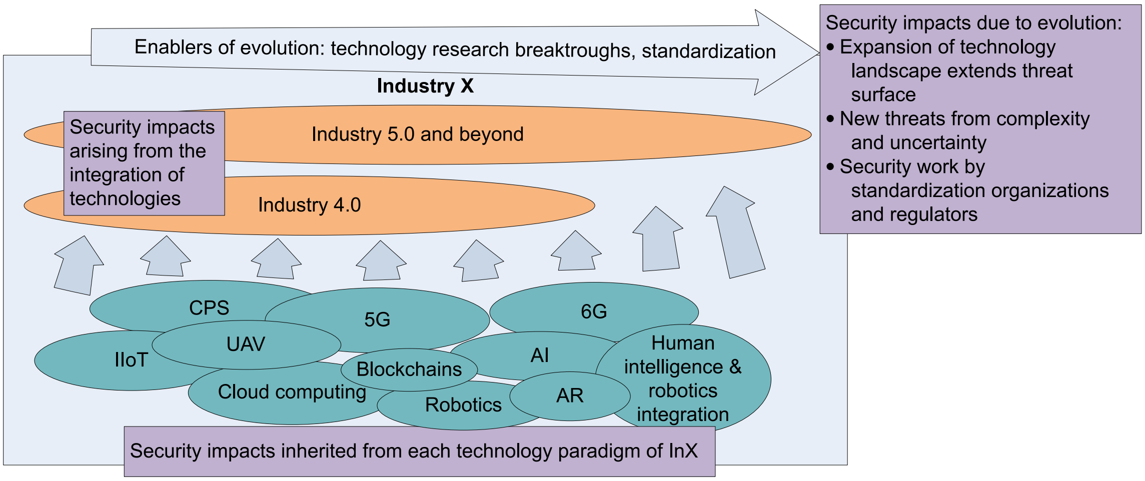
Enablers of evolution: technology research breaktroughs, standardization
Industry X
Security impacts arising from the integration of technologies
Industry 5.0 and beyond
Industry 4.0
Security impacts due to evolution:
• Expansion of technology landscape extends threat surface
• New threats from complexity and uncertainty
• Security work by standardization organizations and regulators
CPS
5G
6G
IIoT
UAV
Blockchains
AI
Human intelligence & robotics integration
Cloud computing
Robotics
AR
Security impacts inherited from each technology paradigm of InX

FIGURE 2. Scope of the survey: security implications and impacts inherited from different InX technologies, and new security implications arising from paradigm integration and from the technology evolution.

IIoT makes the foundation of many systems and services, however, it has been revealed in many studies that the firmware of the majority of IIoT devices has inherent weaknesses that can be exploited for security attacks, as discussed in Section IV. Hence, the applications of these technologies in InX necessitate a thorough investigation of the security threat landscape of InX. Therefore, in this article, our main motivation is to investigate the consequential security challenges InX will face due to the integration of such novel technologies, study the potential security solutions, and find the existing security gaps for future research.

B. CONTRIBUTIONS OF THIS ARTICLE

- In the evolution towards InX, what are the most important technological enablers of InX that rely on communications networks and technologies?
- Since communications technology will make the backbone of most enabling or supporting technologies of InX, what will be the most important security challenges (weaknesses and threats) to those technologies and the overall InX ecosystem?
- What are the potential security solutions for those security challenges in each of the enabling technologies?
- What are the main standardization efforts in the realm of security of those enabling and supporting technologies of InX?
- What are the main existing security gaps that require further research?

In this article, the emerging security challenges in communications of technologies of InX are identified, discussed, and evaluated to motivate future research in this direction. First, the main technologies used to enable InX are highlighted. Then their security weaknesses are discussed based on recent state-of-the-art research work. Furthermore, the potential security solutions and technological concepts are presented. Future research directions are drawn to grasp the attention of researchers to the existing security challenges.

This article is organized as follows: Section II presents the related work, focusing on the existing survey and review articles that either focus on the security of Industry 4.0, Industry 5.0, or the important technological enablers of InX. Section III provides a brief introduction to the key enabling technologies of InX. The section also gives a glimpse of the importance of security of the overall ecosystem, as well as the key enabling technologies. Section IV focuses on the security of communications networks and technologies in InX. Section V discusses the security of the selected technologies in the industrial infrastructure technologies, such as IIoT, CPS, and robots, etc., and Section VI details the security of industrial applications with examples of augmented reality and blockchain. Risk management and standardization efforts are elaborated in Section VII. Important insights and lessons learned are discussed in Section VIII. Future research directions are presented in Section IX, and the article is concluded in Section X. For smooth readability, the organization of the survey is depicted in Fig. 3, and the most used acronyms are presented in full form in Table 1.

II. RELATED WORK

Due to the increasingly critical nature of operations of future industrial systems, huge research efforts are underway on various aspects of its security. Most research efforts focus on specific themes that can be counted within the boundaries of InX. However, there are limited efforts that present security challenges and possible solutions in communications of industrial systems as a whole. Since, InX uses several technologies that rely on communications, such as IIoT, CPS, machine learning, big data, and unmanned aerial vehicle (UAV), to name a few, its security has become highly complex. This complexity can be the main reason for limited efforts in presenting security challenges and possible

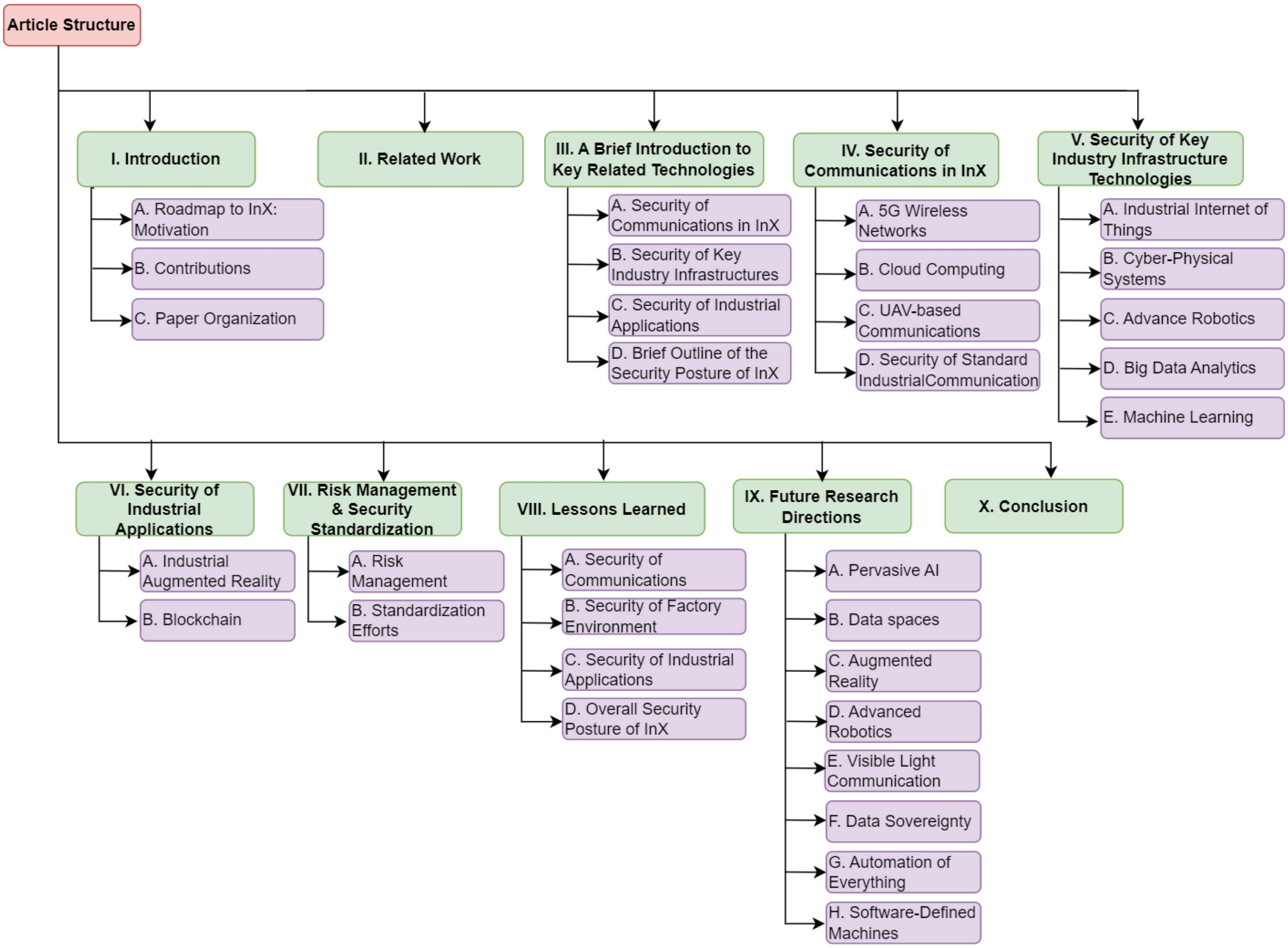
Article Structure
I. Introduction
A. Roadmap to InX: Motivation
B. Contributions
C. Paper Organization
II. Related Work
III. A Brief Introduction to Key Related Technologies
A. Security of Communications in InX
B. Security of Key Industry Infrastructures
C. Security of Industrial Applications
D. Brief Outline of the Security Posture of InX
IV. Security of Communications in InX
A. 5G Wireless Networks
B. Cloud Computing
C. UAV-based Communications
D. Security of Standard IndustrialCommunication
V. Security of Key Industry Infrastructure Technologies
A. Industrial Internet of Things
B. Cyber-Physical Systems
C. Advance Robotics
D. Big Data Analytics
E. Machine Learning
VI. Security of Industrial Applications
A. Industrial Augmented Reality
B. Blockchain
VII. Risk Management & Security Standardization
A. Risk Management
B. Standardization Efforts
VIII. Lessons Learned
A. Security of Communications
B. Security of Factory Environment
C. Security of Industrial Applications
D. Overall Security Posture of InX
IX. Future Research Directions
A. Pervasive AI
B. Data spaces
C. Augmented Reality
D. Advanced Robotics
E. Visible Light Communication
F. Data Sovereignty
G. Automation of Everything
H. Software-Defined Machines
X. Conclusion

FIGURE 3. Organization of the article.

solutions for the whole InX ecosystem. In this section, we provide a brief literature review of existing surveys and review articles on the security of InX, and/or technologies that are highly related to InX from the communications perspective. The most relevant recent articles are highlighted in Table 2. The main theme of the article is tick-marked (✓) concerning the relevant technology. As an example, the first article in Table 2, Overview of Industry 4.0, focuses on CPS, and thus there is (✓) under CPS.

A survey on opportunities and challenges existing in Industry 4.0 is presented in [3]. The authors emphasize on mobile Internet, IoT, CPS, cloud computing, and big data as the most important enabling technologies. Among the vital challenges are the development of smart devices, the construction of a network environment for CPPS, the integration models for CPS and CPPS into a homogeneous environment, and the lack of verification and testing platforms for CPS. A survey on the security of Industry 4.0 from the aspects of edge computing and blockchain, mainly to secure IIoT-based critical infrastructure, is presented in [58]. The main focus of the article is on the convergence of edge computing and blockchain for scalable security of critical infrastructure.

A detailed account of security challenges in Industry 4.0 is presented in [43]. The main design principles pivotal to Industry 4.0 are interoperability, information transparency, technical assistance, and decentralized decisions. Each of these design principles will attract new security challenges when converged to practicality in future industries since new technologies attract new types of attacks. Security attacks can include simple that can be mitigated with simple techniques as well as complex attacks that can circumvent the functionality of the whole system. Various attacks are highlighted on different enabling components of Industry 4.0 such as CPS, IoT, cloud infrastructures, Industrial Control Systems (ICS), and the flow of goods and information. The authors also outline security design principles that are relevant to each underlying enabling technology.

Conti et al. [59] provided a review of ICS designs, devices, and security protocols, and evaluated their robustness over existing ICS testbeds and datasets. It also offers recommendations for their design and reports on the top-performing algorithms. The survey in [60] examines how ICS has developed from standalone setups to cloud-based settings, emphasizing how these technologies are convergent with the

TABLE 1. List of most common abbreviations.

Acronym	Full term(s)
5G	Fifth Generation
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AR	Augmented Reality
BAN	Body Area Network
CCPS	Cyber-Physical Production Systems
CPS	Cyber-Physical System
CSI	Channel State Information
D2D	Device to Device
DLT	Distributed Ledger Technology
DPI	Deep Packet Inspection
DRL	Deep Reinforcement Learning
ECC	Elliptic Curve Cryptography
eMMB	enhanced Mobile Broadband
ETSI	European Telecommunications Standards Institute
GCS	Ground Control Station
ICS	Industrial Control System
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
InX	Industry X
IIoT	Industrial Internet of Things
IoT	Internet of Things
LWPAN	Low Power WAN
MEC	Multi-access Edge Computing
MIMO	Multiple Input Multiple Ouput
mIoT	massive IoT
mMTC	massive Machine Type Communication
NFV	Network Function Virtualization
NLP	Natural Language Processing
PaaS	Platform as a Services
pls	Physical Layer Security
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
RFID	Radio Frequency Identity
RSA	Rives Shamir Adleman
RSS	Received Signal Strength
RTT	Round Trip Time
SCADA	Supervisory Control and Data Acquisition
SDN	Software Defined Networking
UAV	Unmanned Aerial Vehicle
uRLLC	ultra-Reliable Low Latency Communication
UWB	Ultra Wideband
V2V	Vehicle-to-Vehicle
VNF	Virtual Network Function
VR	Virtual Reality
VP	Virtual Private Network
WSN	Wireless Sensor Networks

Internet. The study places particular emphasis on the application of machine learning techniques to improve cybersecurity in the context of cloud-based industrial process migration. The recently published survey in [55] highlights the growing necessity for customized cybersecurity measures in ICSs by highlighting complex and individualized attacks on key infrastructures. Here, the authors examined the benefits of Software-Defined Networking (SDN) in creating coordinated intrusion response plans for ICS and provided a taxonomy of intrusion response plans. The adaptation of threat modeling for ICSs is summarized by Khalil et al. [56] through comprehensive literature evaluation, provided their vulnerability to cyberattacks that can have severe consequences. The study emphasizes the significance of strategic frameworks covering security, privacy, and improved validation metrics in ICS threat modeling approaches.

Supervisory control and data acquisition (SCADA) systems have become an integral part of modern ICSs. SCADA [61], [62] are ICS used to monitor and control critical distributed systems that span large geographic areas. Examples of such systems include electric power transmission and water distribution systems, and facilities in single sites such as manufacturing industries. A survey on the security of SCADA systems is presented in [47]. The survey presents protocols, security threats, and possible solutions to those threats. Another survey on the security of SCADA systems [63] discusses various attacks and countermeasures. However, there is no survey, at the time of writing this article, that directly addresses different aspects of security in InX. Therefore, we also present survey articles that cover the security of each of the most important technologies to communications in InX.

Since 5G is considered one of the main technological enablers of reliable communications in InX, the security of 5G will have strong implications for InX. The security challenges in 5G with possible solutions and future research directions are presented in [22]. Since 5G is a conglomeration of several technologies, including 4G technologies, the security of 5G is highly dependent on those technologies. For example, network function virtualization (NFV) [64] and the concepts of software-defined networking (SDN) [65] have their own security implications [8], [66], and thus these technologies must be properly secured to ensure the security of 5G. Furthermore, due to the conglomeration of new devices (e.g., IoT) and services (5G verticals), security monitoring must be automated due to the resulting humongous growth in network traffic. Therefore, authors in [22] discuss the need for machine learning-based automated security systems that can also predict outage or failure of different technologies and segments of the network. However, there is no visible work, at the time of writing this article, on reviewing the security implications of 5G networks on InX or even Industry 4.0.

A detailed discussion on the enabling technologies, applications, and challenges of the industrial Internet is presented in [28]. The article discusses the security of the industrial Internet from the perspectives of industrial terminal security, industrial data security, industrial communication security, and industrial management security. Communication authorization and data encryption have been considered to be the most important security concerns. A survey on Information and Communication Technologies (ICT) for Industry 4.0 is presented in [40]. The article highlights the security challenges that can arise from the integration of different technologies in Industry 4.0 such as IIoT and cloud computing.

A detailed survey on IoT-induced security vulnerabilities in critical infrastructures is presented in [34]. The authors discuss how malicious actors exploit weak IoT technologies as a first step toward compromising critical systems connected to those IoT devices. The article [34] further explains the security challenges caused to other industrial systems including smart grids, smart homes, and building automation systems, and also highlights the

TABLE 2. Existing survey and literature review articles with main focus highlighted and compared to our article.

Pub. Year	Reference	Focus	Relevant technology covered									
			5G	CPS	IIoT	BD	ML	CC	Rob	UAVs	AR	BC
2015	[3]	Overview of Industry 4.0		✓								
2016	[24]	Industrial WSN architectures and protocols		✓	✓							
2017	[25]	ML and BD techniques for IoT			✓							
2017	[26]	Cyber physical system security		✓								
2017	[27]	Wireless security for CPS and IoT		✓	✓							
2017	[28]	Industrial Internet	✓		✓	✓						
2017	[29]	Industrial augmented reality									✓	
2017	[30]	Security trends and advance in Industry 4.0		✓	✓	✓		✓				
2018	[31]	Security of ML techniques and algorithms				✓	✓					
2018	[32]	ML for IoT (sensor networks) security			✓							
2018	[33]	Survey on IIoT and its challenges			✓							
2018	[34]	Survey on IoT-induced vulnerabilities			✓							
2018	[35]	Security in distributed robotic frameworks							✓			
2018	[36]	Security of Industrial CPS		✓								
2019	[37]	Vulnerabilities in IoT		✓	✓							✓
2019	[22]	Security challenges and solutions in 5G	✓					✓				✓
2019	[38]	Security challenges and solutions for IoT			✓							✓
2019	[39]	Data management in Industry 4.0				✓			✓			
2019	[40]	Survey of ICT for Industry 4.0										✓
2019	[41]	Cloud robotic environments						✓	✓			
2019	[42]	Security of UAVs	✓							✓		
2019	[43]	Security challenges in Industry 4.0		✓	✓	✓		✓				
2020	[44]	Security challenges and solutions for IIoT			✓							✓
2020	[45]	Security for IoT & IIoT using blockchain			✓							✓
2020	[46]	Security of machine learning in industry					✓					
2020	[47]	Security of SCADA systems, mainly protocols		✓	✓							
2020	[48]	Edge computing in IIoT	✓		✓			✓				
2021	[49]	Security of IoT, IIoT, and CPS using honeypots		✓	✓							
2021	[50]	DoS and deception in industrial CPS		✓								
2022	[51]	Attacks and incidents in industrial CPS		✓	✓							
2022	[52]	Blockchain security enabler for Industry 5.0		✓	✓			✓		✓		✓
2022	[53]	Cybersecurity awareness in IIoT		✓	✓							
2023	[54]	5G deployment challenges in automation	✓	✓	✓							
2023	[55]	SDN approaches for intrusion response in ICS	✓	✓	✓		✓					
2023	[56]	Threat modeling of ICS for threat mitigation		✓	✓	✓						
2023	[57]	IoT security challenges in automation systems		✓	✓							
2024	**Our article**	Communications Security in InX	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

*BD: Big Data, ML: Machine Learning, CC: Cloud Computing, Rob: Robotics, BC: blockchain.

possible mitigation techniques. In [45] the authors focus on the security of several IoT/IIoT applications by classifying threats according to the object of vulnerability, either software, network, or data. Also, the role and importance of blockchain (as well as its limitations) in IoT/IIoT security are highlighted, and use cases such as E-Healthcare, VANET, supply chain, and smart grids are discussed. Issues like reducing blockchain feedback latency and computation overhead, and the need to develop application-specific security approaches are mentioned as open research areas.

A survey of IIoT is presented in [67]. The article provides a state-of-the-art study on IoT and its relation to industry. Challenges, opportunities, and future research directions in IIoT are presented in [33]. A survey on threats to IoT is presented in [38], where besides threats to IoT on the general level, a comprehensive attack methodology for malware attacks is presented. Persistent attacks include node compromise and malware attacks which are attributed to weaknesses in communication protocols. Similarly, centralized control architectures can be detrimental because of a single point of failure. Furthermore, a systematic survey on the security of

IIoT with requirements and opportunities presented by fog computing is provided in [44]. IoT security is one of the biggest weak points that holds back the adoption of IIoT, mainly because of poor security resulting in globally known compromises in industrial systems [44]. A survey of practical security vulnerabilities in IoT is presented in [37] and [57]. The latter article also addresses the general challenges the IoT philosophy creates in structures automation systems.

The CPS security is often seen as overlapping with IoT security [68]. Therefore, threats and defenses for wireless connectivity for IoT and CPS have been surveyed together, e.g., in [27]. The differences in the concepts [68] lie in the emphasis: while IoT emphasizes identification and Internet connectivity for all kinds of devices, the CPS concept emphasizes monitoring, control, and automation of physical processes without referred connectivity protocols. Security threats and solutions for CPS have been surveyed in [26]. Similarly, a survey on security control and attack detection in industrial CPS is presented in [36]. The work presents a security overview, keeping in view the limitations of resources of CPS for security, from control theory perspectives. The main challenges, such as DoS, replay, and deception attacks, are discussed from the engineering perspective. Furthermore, the approaches of using honeypots and honeynets for the security of IIoT and CPS are presented in [49]. A comparative examination of protocols and architectures of industrial wireless sensor networks (WSNs) from the perspectives of existing standards is presented in [24].

A survey on data management in Industry 4.0 is presented in [39], where the article discusses security laps in the technological enablers of assembly lines and industrial robots. Here, the distributed systems to avoid sending data over insecure channels and single points of failure, are suggested to be adopted. Furthermore, the article [39] highlights that real-time security systems are required that detect abnormal behaviors early on to avoid the cascade of failures throughout the whole system.

Authors in [69] present the applications of digital twins and big data in the smart manufacturing process, for carrying out predictive maintenance, design of products, and planning during the production process. Müller et al. [70] illustrated the relationship of an industry encountered with big data analytics, in which the economic study helps to analyze the magnitude, direction, and impact of their relation. It helps to provide robust business value by marking out vital boundaries by providing empirical evidence. CPS research trends related to big data in industry 4.0 along with cloud computing are investigated in [71]. In a smart manufacturing process, profit per hour is assessed in production processes as a control parameter [72]. It helps to achieve better throughput, yield, and optimal decisions and provides good benefits using advanced algorithms on industrial big data.

There are several survey articles on the security of cloud computing [73], [74]. Related to the security of cloud platforms and the security of information or data on the cloud platform, authors in [75] survey blockchain technologies to improve the privacy and security of cloud platforms. A survey on isolation techniques in cloud data centers that can be crucial to InX is presented in [76]. A systematic survey on the opportunities that fog computing brings to secure industrial systems is presented in [44]. Fog nodes can be used to effectively isolate infected nodes, whereas the rest of the industry can perform normally. Similarly, fog nodes can perform localized monitoring processes, provide on-premises authentication and access control, and perform time-sensitive tasks. Therefore, fog computing can improve the resilience of industrial systems [44]. A survey on edge computing in IIoT is presented in [48]. The article elaborates on the motivation for using edge computing for IIoT, the research progress in this direction, and then highlights the potential challenges. The main benefits, outlined in the article, include improving the system performance, protecting data security and privacy, and reducing operational costs in IIoT environments.

A survey on machine learning methods for the security of industrial protocols is presented in [77]. Since the main focus of the article [77] is on the protocols, the security weaknesses in many protocols are exposed. The authors provide methods of machine learning that are most helpful in analyzing the security of protocols in ICS. A survey of machine learning techniques used in the analysis of security and stability of power control systems is available in [46]. The article highlights studies on various types of machine learning techniques in this regard and discusses their strengths and limitations. The security challenges and possible solutions for machine learning in communication networks are presented in [78]. Big data analytics, machine learning, and the applications of artificial intelligence in wireless networks are discussed in [79].

Security issues in cloud robotics environments are surveyed in [41]. The authors discuss cryptographic algorithms such as Rives Shamir Adleman (RSA), Advanced Encryption Standard (AES), or Elliptic Curve Cryptography (ECC), as options for enhancing security against threats such as network or data storage attacks. Research work in authentication is identified as the starter point of extended research toward the next security phases. In [35], the authors perform a study of the most common middleware used by robotics frameworks, their cybersecurity capabilities, and the impact of security on communications performance. Results show there is no significant effectuation in terms of latency and packet loss. Security of UAVs is studied in [80], the authors cover security threats such as jamming or spoofing as potential threats. Also, basic use cases related to physical layer security (PLS) are mentioned. The authors in [42] focus on PLS as an approach for avoiding eavesdropping attacks and thus enhancing security on UAVs. Technologies such as multiple input multiple outputs (MIMO) antenna and mmWaves are also considered to improve security alongside spectral efficiency.

The work in [81] focuses on the weaknesses of UAVs for civilian and military use cases, as well as countermeasures for efficiently avoiding their exploitation. Among the vulnerabilities discussed, we find user-level vulnerabilities, drone vulnerabilities, and wireless vulnerabilities. In [82], the authors focus on the lack of security mechanisms in widely used UAV and ground control stations (GCSs) communication protocols. Different vulnerabilities are identified, among them integrity attacks, availability attacks, as well as authenticity attacks. The authors in [83] scanned the whole IPV4 address space looking for visible ROS services, they were able to obtain readings and manipulate a robot located in a remote laboratory as proof of the vulnerabilities of robot systems. Also, some recommendations regarding the use of firewalls, VPNs, and exposure limitations are provided. The work in [84] focuses on describing the different vulnerabilities present in robot systems, from physical vulnerabilities to communication and even software vulnerabilities. Also, the authors propose solutions to mitigate possible attacks, including designing for security, the use of encryption for secure communications, and the detection of security breaches.

A review of AR systems in Industry 4.0 with a use-case of the shipyard is given in [85]. The principles of Industry 4.0 are discussed to pave the way for future digital shipyards, termed Shipyard 4.0. Cloudlets and fog computing nodes are suggested for use in the shipyard, similar to Industry 4.0, to minimize the latency and accelerate rendering tasks while offloading heavy computation tasks from cloud platforms. The security of IAR is considered to be important, however, not discussed. Several security risks, potential solutions, critical assets and goals, and sensitive IAR applications are discussed in [29]. Auto-Identification (Auto-ID) and traceability technologies for Industry 5.0 are discussed in [86]. The main focus of the article is on

Different surveys discussing various security services offered by blockchain technology are covered in [87], [88]. Blockchain-based security in the domain of industry 4.0 applications (e.g., smart manufacturing, smart grids, smart vehicles) are presented in presented in [89], [58], [90], [91]. However, despite their growing popularity due to several key features such as decentralization, immutability, and transparency, there are still several security threats in blockchain that must be resolved before its complete adoption in various industrial and manufacturing applications [92], [93]. In this context, the authors in [94], [95], [96] explored various attacks on the blockchain network and possible countermeasures from various perspectives, i.e., threats to the network, attacks on consensus mechanism, and smart contract vulnerabilities. A review of blockchain-based solutions for industry 4.0 is presented in [97], which also provides an overview of using blockchain to provide security solutions.

On a holistic level, the security trends and advances in manufacturing systems in Industry 4.0 are described in [30]. The three main security requirements based on which various solutions and proposals are evaluated are confidentiality, integrity, and availability. The article discusses the security implications on a general or high level, without going into details about the security of each enabling technology. Furthermore, the 5G infrastructure which is considered one of the main enabling technologies of future industries, as elaborated in [11], is not discussed in depth to understand its security implications. For example, 5G can expose factory information through shared cloud environments or provide means for the propagation of security vulnerabilities into the industry.

III. A BRIEF INTRODUCTION TO KEY ENABLING TECHNOLOGIES

InX represents a highly complex environment due to the amalgamation of huge number of diverse sets of technologies with unique requirements. For example, massive numbers of IIoT will be used and, generally, IoT applications have different requirements. Some IIoT applications require high reliability and availability, whereas, some applications require high throughput and low latency [98]. The priorities of throughput or latency might even change over time. Therefore, AI with its disciplines will be a major enabler of the applications and technologies of IIoT [99], [100]. Since IIoT will generate massive data, big data analytics [101] and AI will play a major role in learning the behavior and needs of IIoT and allocate the resources accordingly. For connectivity, different communication technologies will be used, leveraging the latest developments in networking such as SDN, NFV, and MEC [102], [103], for instance, to allocate the necessary resources dynamically.

All of the integrated technologies of InX will have very distinct and unique, security requirements, challenges, and solutions. In this section, we aim to provide a high level overview of the security posture of InX. The InX ecosystem is presented in Fig. 4 that comprises i) secure communications, that connects all the components within InX, ii) secure factory environment, that is composed of different enabling technologies that empower the very functionalities of industrial systems, and iii) industrial applications, that are used between different industrial systems and external stake holders with two specific examples of Augmented Reality (AR) and blockchain. In the following subsections, we briefly discuss these as an introduction for the security analysis.

A. SECURITY OF COMMUNICATIONS IN INX

The backbone of InX is communication technologies that enable the diverse set of industrial systems to work in unison. The main differentiating factor in InX and other industrial revolutions is the capabilities of devices to interact with each other through communication technologies. Therefore, the security of communications technologies is extremely important. The important technologies that are covered under secure communications include 5G wireless networks, since 5G is poised to connect future industrial systems. We also discuss cloud computing under communications security mainly due to its vital role in bringing communications-specific technologies, such as core network functions, into critical infrastructures to meet its unique demands. The

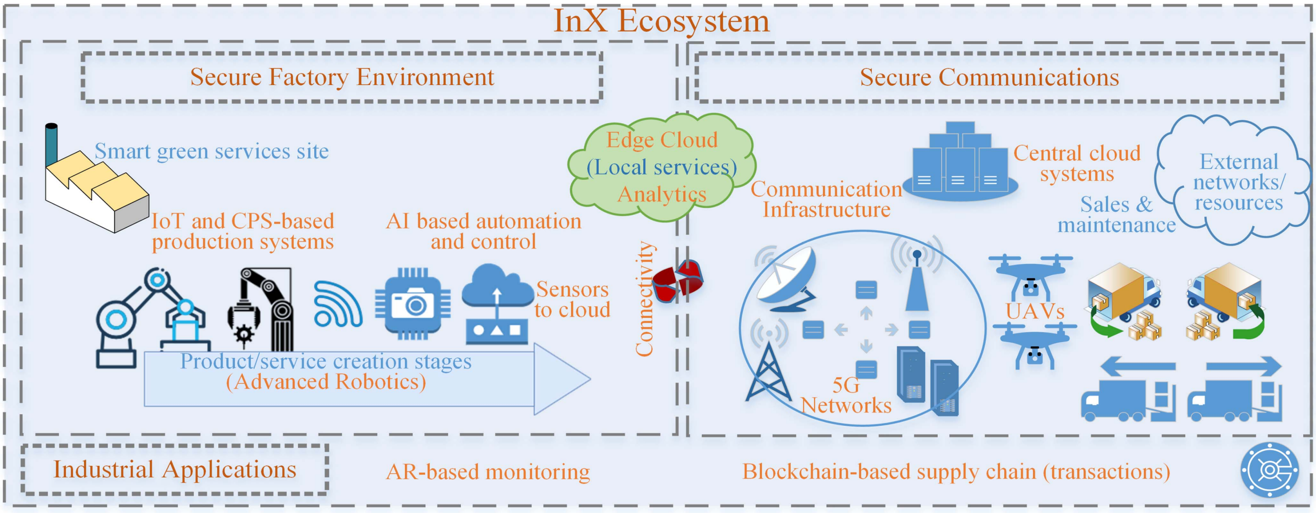
InX Ecosystem
Secure Factory Environment
Secure Communications
Smart green services site
IoT and CPS-based production systems
AI based automation and control
Edge Cloud (Local services) Analytics
Communication Infrastructure
Central cloud systems
Sales & maintenance
External networks/ resources
Connectivity
Sensors to cloud
Product/service creation stages (Advanced Robotics)
UAVs
5G Networks
Industrial Applications
AR-based monitoring
Blockchain-based supply chain (transactions)

FIGURE 4. Simplified visualization of InX integrating factory and external environments.

extension of clouds, such as edge computing, may well be part of the critical factory environment due to its role in data analytics and machine learning, however, we discuss all these concepts together in cloud computing for smooth readability. Furthermore, UAV-based communications and standard industrial communications technologies are also discussed under secure communications.

1) 5G WIRELESS NETWORKS

The existing wired systems, even including the latest technologies, cannot meet the requirements of InX due to the mobile, remote, and dynamic nature of functions and services of InX. Wireless control of industrial processes, on the other hand, requires an ultra-fast, secure, and always-available (five-nines availability) underlying communication system. Since InX requires connectivity of its systems beyond the traditional restricted short-range communications, for example in the supply and demand chain, as highlighted in Fig. 4, cellular networks have become a necessity for industrial technologies [104], [105]. 5G, in this sense, is becoming one of the main enablers of industrial automation [6], [106] with new disruptive technologies that fulfill the requirements of InX. For instance, 5G can serve InX components and services that need extremely low-latency communication, such as the operation of robotic arms, using Ultra-reliable low latency communication (URLLC) [107], [108], and through the migration of critical services or control functions to the vicinity of InX, to edge and fog nodes. Cloud-based systems can also help in separating automation functions from the traditional specialized physical equipment to help increase flexibility and agility [11]. Since cloud computing has become increasingly important in enabling latency-critical services, cloud computing is also discussed in the realm of secure communications, even though cloud computing is also critical to the factory environment for various functions such as data analysis.

2) CLOUD COMPUTING

Benefiting from higher computing and storage resources, cloud computing and its extension in the form of edge and fog computing, can bring elasticity to InX. Multi-access Edge Computing (MEC) is a standard solution by the European Telecommunications Standards Institute (ETSI) for edge computing [109]. The concept of edge computing has been further pushed towards the local environment to meet even stricter latency requirements, for example, to facilitate lightweight microservices, i.e., nanoservices [110]. Cloud computing is pivotal to InX because of its main role in other enabling technologies of InX such as machine learning and big data analytics, CPS and IoT, and linking other physical objects or systems to services [12]. The main delivery mechanism of data between the local, edge, and remote clouds, as well as between IIoT or CPS and clouds, is considered to be advanced wideband cellular networks [39], such as 5G.

3) UAV-BASED COMMUNICATIONS

With the adoption of smart factories (Industry 4.0) and the envisioning of the InX paradigm, alongside the vast deployment of sensors and actuators, production systems need an efficient optimization of data transmission, low-latency computation, and dynamic decision-making. InX use case scenarios will rely on UAVs for providing ubiquitous wireless connectivity, and efficient in-network computation capabilities that allow the processing of sensory data on time. UAVs will be mainly deployed as aerial base stations or relay nodes for enhancing coverage, capacity, and reliability. Furthermore, UAVs can be deployed as flying mobile terminals for enabling real-time video streaming for generating situational awareness, item delivery or infrastructure inspections, and sensor monitoring [111]. UAVs will also have an important role in supply-chain management in InX.

4) STANDARD INDUSTRIAL COMMUNICATION TECHNOLOGIES

There is a wide array of standardized industrial communication technologies. For example, there are different standards for communication between different IIoT devices, communication technologies for industrial automation, wired communications, and time-sensitive communications. Examples of these standard communication technologies include Message Queuing Telemetry Transport (MQTT), Advance Message Queuing Protocol (AMQP), Constrained Application Protocol (COAP), and ISA100 Wireless, to name a few. These technologies fall in the realm of a secure factory environment, for instance between IIoT devices and production lines. However, for smooth readability, we briefly discuss these technologies in the section on secure communications. Below we describe the most important communication-relying technologies in the secure factory environment.

B. SECURITY OF KEY INDUSTRY INFRASTRUCTURE TECHNOLOGIES

The factory environment is a main industrial site where the actual industry-related functions, such as production, happen. Various technologies are highly intertwined with each other. For example, IIoT and CPS-based production systems, AI-based automation and monitoring, and advanced robots that collaborate for production, as shown in Fig. 4. Below, we briefly outline the importance of these technologies in InX along with their security.

1) IIOT

Beginning with an abstract idea of cost-efficient tagging and tracking of "things", which we use daily, IoT started its movement of towards its current use and future visions [112]. Currently, IoT technology has become such an important aspect of future societies, that the success of future connectivity infrastructures, such as 5G, is tied to the widespread use of IoT, resulting in the enormous growth of the IoT landscape [102]. The industry of the future is no different, where devices and equipment ranging from tiny to powerful industrial systems and applications will rely on IoT [67]. IoT will facilitate pervasive or ubiquitous computing by bridging the gap between digital and physical existence through low-cost, low-power, and easy-to-deploy digital devices [113], [114], [115]. IoT in the sense of InX is the collection of sensors, actuators, robotic arms, and other mechanical components having the capability to send or receive data over the network or Internet, making also Industrial IoT or IIoT. IIoT has to be defined in [116], from which we take the bottom line: IIoT works to optimize the overall production value of industries. IIoT has, thus, become a backbone of InX, and several proposals exist for improving the performance of IIoT in Inx [117].

2) CPS

CPS bridges the gap between physical computing and communication infrastructures. The gap is already shrinking as envisioned by smart and gadget-free computing environments [118], and research has been initiated on the security of such environments [119]. The concept of CPS is an enabler for automation and it emphasizes control and sensing technologies as well as machine-to-machine communication. CPS enables close interactions of computation and physical processes, typically with a feedback loop and often without direct human involvement. Examples of industrial processes, where physical processes are sensed and actuated by controller software, include, e.g., smart grids, autonomous vehicles, robotic systems, nuclear power plants, as well as control systems for dams, oil, and gas industries. CPS, thus, exposes expensive and critical physical assets, processes, as well as sensitive information to the vulnerabilities and threats coming from the cyber-world.

3) ADVANCE ROBOTICS

Robots have been an important part of automation systems, often synonymous with automation, and constitute the key building blocks of future industrial systems [120]. Smart robots designed for performing complex tasks can sense, process, and interact with their environment, improving the state of industries by bringing extreme precision into play [121]. Robot systems are present in a wide variety of use cases, from automotive, aerospace, and defense, to pharmaceutical, and distribution centers, as well as food and beverages industries. Moreover, as connectivity increases, the originally isolated robot systems are being exposed to either corporate networks or the Internet, making them valuable for collecting data and performing analysis on quality, reliability, and productivity.

4) BIG DATA ANALYTICS

Big data is one of the pillars of InX, with smart connected machines playing a predominant role in big data generation [122]. Due to the increasing number of smart devices in InX, some produce bursts of data while others sporadically few bytes, the data will be big, and therefore analytics for such big data will be inevitable to learn and act intelligently in the future. The paradigm shift of industrial transformation towards InX, aided by industrial big data is gaining momentum at a different pace in different parts of the industry. Big data, mostly the combination of structured, semi-structured, or unstructured data is collected from organizations for carrying out predictive modeling and analytics. Big data could be acquired from business transactions, customer databases, social networks, industrial data, and many other sources. There are no definite numerical standards to define the term big, but big data is often characterized by 8 Vs: Volume, Velocity, Variety, Veracity, Value, Variability, Validity, and Visualization as shown in Fig. 5, typically referring to terabytes, petabytes, and exabytes of data. Big data is used in real life to create new value for the

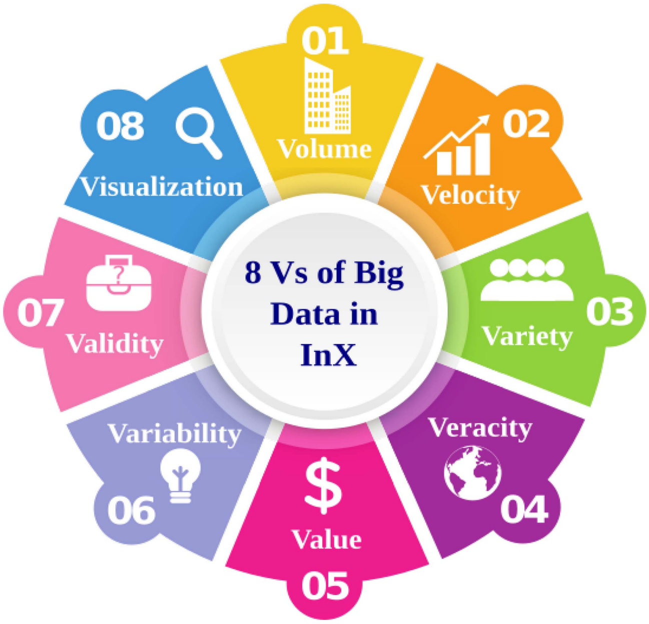

FIGURE 5. Characteristics of Big Data with 8Vs that support InX big data management.

industries and the customers utilizing the products from those smart industries. The trustworthiness of the data, its business value, and the variability of ways the business can use and format the data tailored for end applications play a crucial role in big data. When big data is deployed correctly with appropriate models, it helps industries to improve operations, enhance customer service, create personalized campaigns for marketing products, and improve the profitability of their ventures.

5) MACHINE LEARNING

Machine learning has become a critical technology with its tools to predict the future course of actions based on current and past states of systems, as well as, involved human intervention [123]. Since machine-human interaction is central in InX, machine learning is poised to be one of the main enabling technologies, as discussed in [124]. With 5G providing computing and storage capabilities in the vicinity of InX, machine learning in the network edge [125] in InX will be facilitated by 5G [126]. Furthermore, the tools and techniques of machine learning will use the (big) data generated from the components of InX such as CPS and IIoT, the network (5G), and the diverse services, to name a few. The outcome of the machine learning tools and techniques, along with the necessary feedback, will be to enable and improve real-time decision-making, resource and risk management, systems' functions and security monitoring, prediction of workload and manpower, and improving maintenance and supply chain. One of the most important uses of machine learning in InX is related to the prediction of occurrences of events in the future [127].

C. SECURITY OF INDUSTRIAL APPLICATIONS

There can be a huge number of industrial applications in InX. For example, modern healthcare, public transport, and other public infrastructures can be considered as part of InX, as discussed in [128]. However, we focus on two distinct application areas, such as augmented reality and blockchain, that can become integral to any future industrial system or ecosystem when deployed securely.

1) AUGMENTED REALITY

In InX, augmented reality (AR) is a game-changing technology that is transforming maintenance, safety, operations, and training. AR provides realistic environments and scenarios much more than traditional simulation environments. AR projects digital data into the actual world, giving employees real-time insights and direction. With applications ranging from product design, warehouse logistics, immersive training, remote support, quality control, safety enhancement, data visualization, collaborative work, and enhanced consumer experiences, it plays a critical part in InX. Streamlined to the unique requirements of future industrial systems, Industrial Augmented Reality (IAR) streamlines industrial procedures with AR to lower mistakes and boost the output [85]. IAR applications in InX are broad, ranging from manufacturing to assembly operations, an online guidance system for training the operators, and maintenance to human-robot collaboration [129], [130]. Security in data connectivity, device compatibility, and smooth integration with industrial infrastructure are essential for the success of IAR in InX for more effective and efficient operations.

2) BLOCKCHAIN

The InX environment will be a collaborative, intelligent, and connected ecosystem comprising humans, machines, and other stakeholders, such as, service providers, as well as AI-enabled automation. One of the prime requirements will be to establish distributed trust among various entities throughout the whole ecosystem [52]. In this regard, blockchain as a distributed technology can offer immense added value to InX applications by providing a tamper-proof, decentralized, and trustworthy computing platform for multiple involved entities to securely exchange their transnational data and/or share/sell/rent the available resources among each other without the intervention of any trusted third party or intermediaries [131] [132]. Strong defense against cyber threats is facilitated by fundamental features of the blockchain, which include decentralization, data privacy measures, smart contracts for automatic security enforcement, secure identity verification, auditability, and immutable transaction records. Blockchain holds a distributed and shared digital ledger, where information is encrypted and validated by all participants of the network. Hence, blockchain contributes to improved security throughout InX by ensuring supply chain transparency, offering audibility, and traceability, and fostering interoperability among various devices that are logically and geographically widely distributed [133].

TABLE 3. Summary of Security Challenges and potential solutions in enabling technologies.

Technologies in Inx	Security Challenges	Solutions [Reference(s)]
5G	Availability due to latency in backhaul	MEC based service migrations to InX [134], [135], using URLLC [107]
	DoS attacks on centralized control points	Distribution of resources [136], devolving control functions [137]
	Exposed air interfaces	InX components own end-to-end encryption [138], isolation security [134]
Big Data Analytics	Leakage of data	Blockchain with watermark [139]
	Direct (corruption) threats to data	Secure integration of IoT frameworks [140]
	Anomalies in industrial data	Real time processing with ML [141], [142] using SVM, Random forests [143]
Machine Learning	Cascading failure attacks	Real time data security management [39]
	Denial of detection of faults	Deep learning based DoD mitigation [144]
	Adversarial learning and model poisoning	Adversarial training [145], privacy-preserving ML [146]
	Backdoor attacks	Secure aggregation [147], and neural cleanse [148]
	Privacy leakage	Differential privacy [149], and gradient pruning [148].
Cloud Computing	Physical attacks on fog servers	Lattice-based cryptography [150], security agent [151]
	Cache poisoning attacks on edge devices	Semi-surprised learning unknown traffic detection [152]
	Threat to data ownership on edge devices	Edge-native data encryption [153]
Augmented Reality	Eavesdropping attacks	Secure device pairing via out-bound channel [154]
	Voice-Spoofing attacks	Voice liveness detection techniques [155]
	Unauthorized access to sensitive data	Multi-model authentication using bio-metric and localization features [156]
Blockchain	Sybil Attack	Secure consensus mechanism [157], distributed miner monitoring [158]
	Privacy Leakage	Homomorphic encryption technology and zero-knowledge proof [159]
	Eclipse Attack	Anomaly detection approaches [160], [161], Random selection [162]
CPS	Cyber attacks against control systems	Platform security [163], application segregation [164], [165],
	Physical attacks against sensors	Process-specific controls [166]–[169]
	Interfered or leaking feedback channels	Communication security [170], [171], threat detection [172]–[175]
	Heterogeneity leading to complexity	Secure interoperability [176], [177], holistic metrics [178], cyber ranges [179]
IIoT	Eavesdropping & side channel attacks	Encryption coupled with compression techniques [34]
	Manual or physical tampering	Increased segmentation [34], blockchain [180]
	Resource exhaustion attacks	Security-prioritized resource allocation [9]
Advance Robotics	Outdated OS	Security by design [181], continuous software update and upgrade [182] - [183]
	Poorly encrypted data	Improve security of ROS [184], cryptographic methods for confidentiality [185]
UAVs	Data and control channel jamming	Cryptographic techniques, PLS [186] - [187], UAV cooperation [188] - [189]
	GPS spoofing	Signal strength comparison [190], monitoring of GPS identification codes [191]
	Malware infection	Use of secure communication protocols, continuous firmware update [80]

D. A BRIEF OUTLINE OF THE SECURITY POSTURE OF INX

The InX ecosystem is an amalgamation of a large set of technologies. The technologies discussed in the prior subsections rely on communications infrastructure, such as 5G, as their underlying enabling infrastructure. Since communication technologies can be prone to security weaknesses and vulnerabilities, those technologies will likely face security threats. Therefore, a thorough security analysis of the InX ecosystem is needed, which is the main focus of this article. The security analysis is performed under three main parts of the InX ecosystem. These include the i) security of communications technologies, ii) the security of different technologies used in the factory environment, and iii) the security of critical industrial applications. First, the main security challenges for each technology under each category are brought forth, and then potential security solutions for those challenges are researched.

For smooth readability, the most important challenges and their respective solutions are highlighted in Table 3. The left column in Table 3 presents the enabling technologies of InX, the middle column represents the most important challenges, and the last column highlights the solutions with references to articles that provide details about the specific solutions. In the following sections we discuss these security challenges and solutions, beginning from the security of communications in InX.

IV. SECURITY OF COMMUNICATIONS IN INX

In this section we introduce the main communication technologies along with their security footprint. Since, the fifth generation of wireless networks, also known as 5G, is poised to connect and combine most of the industrial systems either through standalone 5G network or non-standalone 5G network, below we discuss the potential of 5G in InX and then discuss the related security landscape.

A. 5G WIRELESS NETWORKS

Since 5G is crucial for InX, its security is even more important. Furthermore, even if there are security challenges within 5G systems, vulnerabilities must not propagate to InX. Therefore, proper measures should be in place to not only stop security threats in 5G and its technological enablers but also mitigate the risks involved with such vulnerabilities. 5G and its key new technologies including cloud platforms (MEC and fog nodes), softwarized and virtual networks, and the techniques of enhanced mobile broadband (eMBB), and URLLC, etc., do have security challenges as discussed in [7], [8], [10], [54]. Therefore, in the following subsections, we bring forth the main security challenges and vulnerabilities in 5G, and the possible solutions for those challenges and vulnerabilities that are most important to InX.

1) SECURITY CHALLENGES

The security challenges in 5G related to InX are multi-dimensional, from threats to traffic flowing through the network to the network entities and components of InX. Industrial traffic can be categorized into two types, i.e., cyclic and acyclic, generated by different sources and with different time requirements [192]. Cyclic traffic, typically, includes fast data exchange between controllers and field devices and the amount of data is usually a few bytes. The data can be sensing values and measurements with stringent latency requirements such as a few hundred microseconds. The acyclic traffic, comprising limited amounts of data, is triggered by unpredictable events such as process alarms. Communication networks introduce delay into the system, as discussed in [193], and can be struck on the delay constraints, as discussed in [194].

One of the main challenges related to meeting the real-time requirements of InX while using 5G will be the delay introduced in the backhaul networks, as highlighted in [194] for routers and switches. Therefore, any security vulnerability that can increase the latency at any intermediate points within 5G will cause availability challenges in InX. Industrial communication systems and their challenges with future research directions covering the need for 5G-based wireless networks are discussed in [192]. An example of industrial network performance is given, which outlines an approximate packet delivery time for wireless networks to be in the range of a few hundred microseconds. With such stringent requirements, any security threat that could exhaust the resources of intermediate nodes, or congest the communication link for a millisecond, will be considered successful.

The very enabling technologies of 5G, such as Software Defined Networking (SDN), NFV, cloud computing, and massive MIMO, for example, have their own security challenges. Pertinent to InX, technologies centralizing control decisions, such as SDN, will cause most challenges in terms of increasing risks related to availability due to security vulnerabilities. For example, SDN centralizes the network control decisions to (even though logically) centralized control planes, called SDN controllers. These controllers have been demonstrated to increase the visibility of network control points, even if physically distributed, due to the very nature of their operation of installing flow rules in the underlying packet forwarding infrastructure [66]. As a result, there can be clear points of interest to be targeted for security attacks, such as denial of service (DoS) or resource exhaustion attacks. In the case of NFV, hypervisors can be targeted for attacks due to being central to the process of virtualization. Other technologically enabling components of 5G such as massive MIMO can be targeted for different types of attacks such as active and passive eavesdropping [195].

5G is also becoming the de-facto standard in terms of enabling connectivity of many other technologies used in InX that have their own security procedures and protocols for connectivity [54]. Examples of such technologies include low-power wide area networks (LPWANs) that enable massive machine-to-machine (M2M) communications for diverse types of IoT. The security challenges in LPWAN are related to the interfaces, air and wired, and the most pertinent one is the air interface between end-user devices and the gateways or eNBs, as discussed in [196]. Since devices in LPWANs have low capabilities, encryption if not provided by the network (5G) will be left to an optional on-demand basis, which can result in security breaches. Furthermore, the challenges are related to the inherent weaknesses of devices making LPWANs, such as devices in the IoT domain, discussed in the IoT Section V-A.

2) POTENTIAL SECURITY SOLUTIONS

The network that serves or connects IIoT devices and networks needs to understand their unique requirements [197], to adjust or configure itself autonomously to fulfill the service requirements. Therefore, the disciplines of AI such as machine learning can be used to enable the network to learn the requirements of IIoT autonomously and adjust itself accordingly. AI and machine learning algorithms in the edge will facilitate quick network response to the needs of IIoT, as described in [198]. The concepts of cloud computing (e.g., MEC) already facilitate the communication networks to fulfill the service requirements of IIoT in terms of providing computing and storage resources near mitigate its challenges of resource constraints. The extreme densification in future wireless networks (e.g., in 5G) [199], with a variety of heterogeneous access networks [200], using new technologies such as massive MIMO antennas [201], millimeter Wave (mmWave) [202], aims to cope with the challenges of the availability in access networks. SDN and MEC are the key technologies to meet the network resource requirements of IIoT [136]. For example, the global visibility of the status and stats of network resources coupled with programmable control provided by SDN enables run-time service migration from clouds to MEC servers or nodes in the environment.

One of the naturally secured approaches taken in 5G, which is highly important for the security of industrial systems and services, is the 5G verticals as outlined in [6]. Using the concepts of virtualization, strengthened by the concepts of NFV [203], the verticals isolate traffic generated from different sources and thus have the capability to ensure end-to-end security of the different industrial processes. Therefore, huge research is going on in this direction, mainly from the perspectives of its use cases in InX, as discussed in [134]. Multi-access Edge Computing (MEC) has been proposed and used in 5G [204] to meet the latency requirements [135], where the different services can be isolated through the concepts of verticals as discussed in [134]. Such solutions along with URLLC systems [107] effectively address the challenges of latency-critical services.

The inherent limitations in the technologies of 5G such as SDN, NFV, and MIMO need to be addressed first in an isolated fashion followed by security hardening of the integrated 5G system [22]. Solutions to the important security challenges of the main enabling technologies of 5G such as SDN, NFV, cloud platforms, massive MIMO, etc., are discussed in [7], [22]. The security of SDN and NFV in the context of IoT is discussed in [205]. The authors outline how the joint use of NFV and SDN complements the existing security approaches of IoT. For example, how a slice (isolated set of programmable resources) can effectively isolate traffic at run time using the programmable nature of the network enabled by SDN. Security challenges related to the centralized control points can be mitigated by devolving the local decision-making to data plane or localized control point elements, as evaluated in [137] for SDN. In terms of security of the radio devices, the nature of massive MIMO, for instance, being used in a vicinity provides enough opportunity to secure it from passive and active eavesdropping and jamming as discussed in [206], [207]. The tunneling beyond the vicinity using IPSec, for instance, can also provide the required security.

The solutions for maintaining critical communication between InX and remote cloud platforms include maintaining redundant links and prioritizing traffic according to the critical nature of the traffic, as discussed in [208]. In the case of network exposures, some of the devices also have their security procedures if the network exposes its traffic for instance in the case of exposed air interfaces for IoT as discussed in the challenges above. For example, Sigfox devices increase the confidentiality of the data through end-to-end encryption as discussed in [138]. However, all the optional choices of security procedures such as security configurations and encryption technologies need to be mandated and brought into use.

B. CLOUD COMPUTING

Cloud computing will empower data-based real-time decisions in InX. Cloud platforms can be either centralized or distributed using platforms such as MEC or fog nodes, each having their own benefits and consequences in terms of security. Similarly, cloud platforms can be shared among multiple users, operators, or services. Such sharing will require the concepts of virtualization to be used. Virtualization will also have its security challenges. Furthermore, remote cloud systems, including centralized and distributed, will also require the underlying communication systems to be secure enough to avoid misadventures in terms of security. Therefore, the security of cloud systems is multi-pronged and has unique challenges and solutions as described below.

1) SECURITY CHALLENGES

Cloud computing has its challenges of availability and security. The connectivity to local (MECs, fog nodes) or centralized cloud platforms will be mainly provided by the latest cellular technologies that have limited coverage areas, whereas routes to data centers may be long, exposing connections to congestion or many other network problems. Cellular networks also have their challenges of security which can expose the systems to further security challenges as discussed in Section IV-A. The main challenges that exist in the cloud, such as weaknesses in isolation and improper management of virtual machines, will also open InX systems to security vulnerabilities, such as DoS, man-in-the-middle attacks, and availability challenges that can disrupt the flow of the InX process. The Federal Office for Information Security of Germany considered virtual machine manipulation and lack of control of user data in the cloud systems among the topmost ten threats to ICSs in 2016 [209].

The requirements for offering services in industry 4.0 as cloud applications are discussed in [210]. The authors outline the requirement of communication links from a smart grid system to a cloud-based monitoring system, highlighting the possibility of link congestion. The data transfer rate needed in smart grids for monitoring the infrastructure, for instance, is at least 500 kbps per node [211]. Such monitoring relies on communication link providers, who may face congestion in their infrastructure without knowing the critical nature of the communication. Therefore, link congestion can, inadvertently, become an availability challenge for security monitoring of critical functions in cloud systems in InX.

IT assets that the extension of cloud computing platforms, such as MEC and fog nodes, need to manage in the context of InX contain not only data, metadata, and software, but also computing, caching, and networking applications. Due to the physical exposure, boundary openness, weak computational capacity, device heterogeneity, and coarse-grained access control of such IT assets, they are threatened by physical security, computing security, communication security, etc. [212]. Compared with cloud computing, edge and fog computing are composed of computation-limited hardware and heterogeneous firmware. Since distributed dge and fog servers are mainly used for processing delay-sensitive and mobile IoT services, most of the computing, caching, and networking resources in distributed edge/fog servers are used for supporting real-time demand response. However, distributed edge/fog servers do not have additional resources to run complex security protection measures, and thus, simple physical attacks [212], [213], [214] can compromise a lot of edge/fog IT assets. Having noticed this, the adversary favors first capturing several edge/fog IT assets and turning them into weapons against upstreaming fog servers [215], [216].

Caching data at distributed fog servers is one of the most popular services in future industries relying on information-centric networking (ICN) [217]. Considering the remoteness and virtual nature of the Internet, the caching strategies and cached data will suffer from various cache poisoning attacks such as cache pollution attacks, cache side-channel attacks, and cache deception attacks [218]. These cache poisoning attacks will result in huge concerns about privacy, security, and trust in content placement, content delivery, and content usage for mobile users, respectively [219]. Another important trend is to deploy SDN on the edge and fog platforms to manage heterogeneous networks and schedule massive traffic more efficiently [220], [221]. In such frameworks, the data plane only needs to transmit data packets and the control plane focuses on generating/selecting reasonable routing paths for each data packet. The attacks on the control and data planes of SDN, as discussed in [66], pose significant threats to such frameworks. By forging some LLDP data packets in the data plane, an attacker can build fake communication links to fool routing algorithms in the control plane to forward packets in the data packets to fake communication links or interrupt fog services [222].

2) POTENTIAL SECURITY SOLUTIONS

Cloud platforms, as in the case of InX, can be used to increase the security of InX beyond the traditional approaches. Coupled with the latest technologies, for instance, virtualization, cloud platforms can be used to separate different services within InX based on the criticality of the service. To deal with security challenges related to the use of cloud computing platforms in future industries, there are many available solutions, which can be divided into three aspects: first, edge data encryption and key management; second, security situation awareness; and third, certified adversarial defense.

To guarantee edge/fog computing security, all data on edge devices must be encrypted [153]. However, resource-limited edge devices usually cannot support long-term protection over periods of ten or more years. Liu et al. [150] proposed the use of lattice-based cryptography to design efficient data encryption solutions for edge computing devices in the post-quantum IoT. However, most of the data on edge devices will not be stored for a long time and a user device often needs to configure multiple security keys or passwords for different applications. To simplify the complex key management scheme, a reconfigurable edge/fog computing security scheme is proposed, which treats edge servers as a new security agent (SA) to execute security authentication and access control [151].

Security situation awareness is proposed to construct a security state map of the atomized IT assets deployed in different edge computing application scenarios. With such a given security state map, security operators can know the attack behaviors timely and configure security strategy flexibly [223]. The key enabling technology of security situation awareness is network traffic analysis. The most popular network traffic analysis technology is deep learning. Known attacks are easy to detect by extracting features and configuring rules. The challenging and hot task is unknown attack detection. Since the unknown attacks have no accurate labels, a semi-supervised learning algorithm is an appreciable method to actively detect unknown attacks [152]. In such a scheme, the deep learning model actively requests annotations for the newly-arrived network traffic. Combined with the decision-making theory, the deep learning unknown attack detection method has good interpretability.

The security risks brought by artificial intelligence should be circumvented through certified adversarial defense. For adversarial attacks, adversarial training is an active defense technique, which requires feeding adversarial examples into the model training procedure. When the new model learns all permutations of the adversary, adversarial attacks cannot fool such a new learning model [145], [224]. Recently, differential privacy technology has been perceived to have the potential to improve the model robustness and prevent deep gradient leakage [149]. The essential of differential privacy is adding Gauss noises or Laplace noises into the inputs, gradients, or weights of the learning model. By assigning different privacy budgets, the trainer can achieve multiple learning models with different robustness levels. For backdoor defense, the most effective method is gradient pruning, whose performance can also be certified by adjusting the number of pruned gradients [148]. Furthermore, machine learning is discussed below.

C. UAV-BASED COMMUNICATIONS

UAVs are pivotal in an increasing number of use cases within Industry 4.0 and InX (as well as for military and civil operations), mainly due to their high mobility in 3D spaces. As UAVs are capable of either autonomous or semi-autonomous operations, they require reliable navigation in the form of control and GPS communications. This characteristic of UAVs makes them the target of attackers trying to hinder their communication links using either simple or well-designed hacks to get their control. Furthermore, UAVs are generally computation and energy-constrained devices, with limitations that hinder the deployment of complex, and upper-layer-based security solutions, which are deemed as computation and energy costly. In the same manner, their high mobility combined with their physical fragility paves the way for new security challenges. Therefore, we discuss the main security challenges and possible solutions for those challenges in the context of InX below.

1) SECURITY CHALLENGES

Jamming is one of the main threats against UAVs as they provide a strong line-of-sight (LoS) in use cases where they act as either a base station, relay node, or flying mobile terminal. Strong air-to-ground (A2G) and ground-to-air (G2A) communication links improve the reception of malicious eavesdroppers as well as ground or aerial jammers, affecting the communications and control channels of the UAV [225]. Jamming uses radio interference to degrade wireless communications by keeping the channel busy, corrupting the signal at the receiver, and causing the transmitter to retreat when sensing the medium is busy. Although jamming attacks mostly target the physical layer, cross-layer attacks are also possible as a jammer can have similar capabilities to the legitimate nodes in the network [189]. By jamming the communications and control channels of a UAV, an attacker would hinder communication with other UAVs and with its remote controller. Jamming the GPS receiver will block the autonomous flight of a UAV [226].

Another important threat is GPS spoofing. In spoofing attacks, signals identical to those of valid satellites are generated by the attacker, the receiver cannot identify the real signal and chooses the counterfeit as valid based on its power [227]. There are two different methods for an attacker to take over a GPS, overt capture, and covert capture. In overt capture, a combination of jamming and spoofing attacks is used, whereas in covert capture the attacker assumes the target possesses spoofing detection measures that must be avoided. The covert nature of GPS spoofing attacks makes them difficult to identify (in comparison with the more obvious jamming attacks) as the UAV cannot verify whether or not the ground station has been compromised. In the same manner, the unencrypted, unauthenticated, and open structure of GPS signals alongside their data bit predictability, facilitates the job of the attacker. When successful, a GPS spoofing attack can grant the attacker total control over the UAV position, velocity, and time [228].

Malware infection is also possible as attackers can exploit the vulnerability of embedded communication protocols through a reverse shell payload that is injected into a UAV's memory and installs malware on the systems running the ground stations. A reverse shell attack consists of a shell session that is initiated from a remote node towards the local machine, they are used by attackers that performed a remote command execution attack as it is the only way to gain remote shell access through NAT or a firewall. This threat is worsened by the applications used for allowing users to pilot UAVs using their tablets or mobile phones as wireless remote controls [80]. A combination of the aforementioned attacks is used to physically affect the UAVs either by capturing, replacement of its cargo, or controlling the drone with the sole purpose of crashing it. These physical vulnerabilities are relevant as drones can also play a logistic role in InX.

2) POTENTIAL SECURITY SOLUTIONS

An interesting approach for jamming protection is PLS, which efficiently protects transmissions between network nodes, hindering the efforts of malicious eavesdroppers. Cryptographic techniques are widely used for protecting data transmission of the UAVs in the upper layers [186], [187]. For protecting the A2G links, some of the techniques used are beamforming, trajectory and communications design, and UAV cooperation. 3D beamforming offers a more refined beam resolution in both elevation and azimuth plane (especially effective when used alongside a noise signal), making it an attractive option for 5G applications, and nulling the user's signal in the directions of eavesdroppers [207]. Efficient trajectory and communications design is aimed at helping the UAV move more freely in the 3D space, avoiding blockage with users and incurring blockage with malicious eavesdroppers, thus improving communications and secrecy rate [229], [230]. UAV cooperation expects to improve the maneuvering limitations of UAVs to increase security performance by deploying multiple collaborative UAVs. In this scenario, some of the UAVs might act as jammers being deployed close to ground eavesdroppers, and degrading their signal quality by sending noise signals [188], [189]. Protection of G2A can be achieved by using the aforementioned techniques, as well as implementing device-to-device (D2D) communications. Frequency-hoping spread spectrum (FHSS) and direct-sequence spread spectrum (DSSS) is some widely applied anti-jamming techniques, although their application is limited due to the strong LoS and a spectrum-efficiency trade-off [231].

There are several effective countermeasures against GPS spoofing and their application depends on the nature of the attack. Techniques useful against basic attacks include the observation and comparison of the received signal strength over time [190], and the monitoring of the identification codes of GPS satellites to check whether they are constant or not [191]. Nevertheless, more experienced attackers can avoid these protective measures as they tend to use sophisticated and more complex attacks. Better planned attacks can be detected by equipping a UAV with two GPS receivers and checking their cross-correlation, however, this method was not efficient against attacks sending weak spoofing signals [228], [232]. A technique proposed in [233] can detect spoofing attacks via a ground infrastructure that checks real-time information regarding the time of arrivals to the expected UAV positions over time, this technique has been quite effective in detecting spoofing attacks within two seconds, and the attacker's location within fifteen minutes of monitoring. In [234], the authors introduce a system dynamics-based framework that includes a cooperative localization-based anti-spoofing mechanism that can determine the real location of an attacked UAV based on the location of neighboring UAVs. Finally, malware infection can be avoided by using secure communication protocols such as eCLSC-TKEM. Also, on the ground station side, privileged access needs to be tightly controlled, avoiding the execution of files from the /temp directory, setting up deep packet inspection solutions intercepting SSL and TLS connection, alongside a continuous update of the firmware to help reduce the possibility of suffering reverse shell attacks [80].

D. SECURITY OVERVIEW OF STANDARD INDUSTRIAL COMMUNICATION TECHNOLOGIES

In this subsection, we briefly discuss the most important standards for industrial communications with their security features. The range of industrial communication systems is very wide and spans almost four decades of evolution [6]. Accordingly, the availability of security features is diverse. Most older field-level communication systems do not provide security at all, which led to the development of defense-in-depth concepts [235]. Modern industrial communication systems based on Ethernet and/or IP lend themselves to the application of security layers known from the IT world.

1) MQTT

MQTT (Message Queuing Telemetry Transport) is a widely used standard for IoT and IIoT (Industrial IoT). MQTT is based on the publish-subscribe model, providing an indirect route, via a broker, between publishers and subscribers [236]. The presence of MQTT is not limited solely to IoT or IIoT, the standard MQTT-SN (MQTT-Sensor Network) offers resource optimization for running on processing and memory-constrained devices by using simpler header and payload structures than regular MQTT [237]. Regardless of its ubiquitous nature, MQTT is vulnerable to security threats as its only security feature is unilateral authentication. It lacks security functionalities such as access control, or control message security. To secure the communications channel, current MQTT implementations make use of TLS (Transport Layer Security) between devices and the broker [238].

2) AMQP

AMQP (Advance Message Queuing Protocol) is a standard for asynchronous message queuing that facilitates the exchange of messages between components of a system, independently of their underlying implementation. The AMQP model is capable of emulating store-and-forward queues, as well as topic subscriptions, or even content-based routing [239], [240]. Although conceived in the financial sector, AMQP is used in a range of challenging applications that include autonomous computing, cloud computing, and IoT. Unlike MQTT which is intended for telemetry transmissions and aims at constrained devices, AMQP can work with both constrained and unconstrained nodes. AMQP implements TLS and SASL (Simple Authentication and Security Layer), including modern SASL mechanisms like GS2 and SCRAM-SHA (Salted Challenge Response Authentication Mechanism). Furthermore, AMQP's design allows for the use of alternative security mechanisms as they are developed [241].

3) COAP

CoAP (Constrained Application Protocol) is a Web transfer protocol that provides a client-server (URI-based) model for connecting constrained application nodes and easily interfacing with HTTP. CoAP is mainly deployed in environments such as smart energy and building automation, since its standardization in 2014 research has shown it is an efficient option for low signal strength environments [242]. Being UDP-based, the networking overhead associated with TCP is avoided, although a UDP-based confirmation and retry model is included to facilitate message delivery. CoAP makes use of DTLS (Datagram Transport Layer Security) to secure the communications channel, it is based on and provides a similar level of security as TLS [243].

4) ISA 100 WIRELESS

The ISA100 Wireless standards aim to be the universal solution for industrial wireless networks. Developed by the ISA100 committee, the standards focus on addressing the requirements of the emerging Industry 4.0, make use of 6LoWPAN (Low-power Wireless Personal Area Network), include specifications regarding protocol stack, system administration, security for low data rate wireless devices, among others. It is also fully compatible with smartphones, as well as IEEE 802.15x, IEEE 802.11x, and IEEE 802.16x devices [244]. In ISA100 Wireless, a security manager entity is in charge of authenticating, storing, and distributing end-to-end security keys. Security options are optional and can be deactivated in scenarios where end devices are constrained, however, this flexibility poses a security threat. One of the standards, the ISA100.11a, uses AES symmetric encryption and provides direct messages in a peer-to-peer fashion, the latest version of the standard provides security spoofing and reply attacks [245].

5) 6TISCH

The Timeslotted Channel Hopping (TSCH) mode was introduced to the Medium Access Control (MAC) portion of the IEEE802.15.4 standard. The TSCH is the standard for industrial automation and process control. The IPv6 over TSCH (6TiSCH) is aimed to enable the adoption of IPv6 in industrial standards. Details about the security of the IETF 6TiSCH are presented in the survey paper [246], which outlines different standards for lightweight industrial communications. The security of 6TiSCH is still under research, where issues such as sharing secret keys among the network nodes are an open question. However, the 6TiSCH architecture defines static scheduling, hop-by-hop scheduling, neighbor-to-neighbor scheduling as well as remote monitoring and scheduling management, where the security demands are high. Their engagement in track forwarding, fragment forwarding, and IPv6 forwarding is highly recommended for low-power industrial communication.

6) ETHERCAT

EtherCAT is an ethernet-based control solution for industrial automation sectors. It is capable of addressing specific concerns in industries such as rapid response times, minimal data requirement for the devices engaged in communication, and efficient cost of implementation. With EtherCAT, the master sends data possibly only a single frame for the entire node network that will pass through each node [247].

However, the EtherCAT protocol lacks connection-based security and flow issues for recognizing the masters and slaves in the network, which may lead to vulnerability in the MAC layers, DoS, and man-in-the-middle attacks.

7) PROFIBUS

The Profibus is one of the most common networks used in the industrial automation process. Such a process field bus, which is meant for interfacing decentralized peripherals, where can drastically reduce the wiring costs. However, one of the serious concerns in the Profibus is the authentication issues among the master and slave nodes in the network [248]. Moreover, they are also susceptible to DoS threats, which need isolation from the other devices in the network.

V. SECURITY OF KEY INDUSTRY INFRASTRUCTURE TECHNOLOGIES

In this section the security of key technologies in industrial environments that rely on communication technologies as their backbone are discussed. For example, IIoT and CPS systems are already integrated into industrial systems for a range of purposes, ranging from controlling large production and assembly lines to actuators in individual components. Similarly, collaborative robots relying on fast communication infrastructure co-work to create or assemble different products. Different industrial processes are monitored through machine learning techniques using huge amounts of data (big data) generated by sensors, IIoT or CPS systems, and communicated to nearby edge clouds or centralized clouds for processing. In the following subsections, we discuss the security of these technologies that make the factory environment and are dependent on communication technologies.

A. INDUSTRIAL INTERNET OF THINGS

The use of IIoT is extremely diverse, ranging from nanochips in healthcare to precision agriculture and monitoring oil pipelines over long distances. In InX IIoT will be used in massive numbers and will be connected through communication networks to enable new services needed by companies such as predictive maintenance of industrial equipment, surveillance, remote control, consumption metering, asset tracking, transport, etc. Since IoT usually have low capabilities in terms of memory and processing [117], the environment in which they operate must provide sufficient security. IIoT devices themselves can have security weaknesses either inherently or can be compromised due to low resources onboard, as discussed below.

1) SECURITY CHALLENGES

There are several challenges to the smooth operation of IoT from various perspectives. For example, the challenges due to the limitations of IoT devices in terms of computing, storage, and communication capabilities [67], [249], and the challenges imposed by the operating environments, such as communication networks [250], [251], that include interference [252], security [253], [254], [255], and availability of network resources. One direct consequence of low resources, discussed in [33], is that IIoT will mostly be not capable to run resource-demanding cryptographic protocols, for instance, based on public-key cryptography. An availability challenge in network access is caused by the higher number of concurrent access to the network, large overhead during synchronization among the devices, and the lack of support for bursty or sporadic arrival of the data from IIoT devices and networks [256].

Security challenges of IoT with some case studies and their potential solutions are discussed in [257]. The article elaborates on attacks due to software failures and vulnerabilities, such as buffer overflows in firmware, or through physical tampering in electronic circuits or memory of physically captured IoT devices, for instance, copying or changing the identifying and authenticating information of devices. Furthermore, the article [257] discusses the possibility of eavesdropping and man-in-the-middle (MITM) attacks to sniff data traffic and extract critical network information in case of the communication lacks encryption. The article also discusses malicious code injection with physical access to IoT devices, for example, in a very simple way by pressing the hard-reset button.

Some of the devices have limitations in terms of bandwidth and thus there is an upper bound on the packet header size leaving little room for additional security-related information [138]. The low header space, low memory, and low processing capabilities make the conventional elliptic-curve or asymmetric cryptography not suitable for such devices. For example, asymmetric cryptography works with keys of bigger lengths than the payload of sigfox [258] of 12 bytes. Similarly, the limited number of message transmissions in Sigfox does not allow the parametric exchanges of the elliptic curve algorithms [105]. The lack of encryption is a major challenge in IIoT communication. For example, most of the control components in field bus communication communicate with plain text, allowing attackers to compromise the systems with little effort, issue control commands, or at least read information [209]. Furthermore, covert channel attacks, exploiting traditional client-server communication approach, over Modbus/TCPIP communication channels is demonstrated in [259]. It has been shown that signaling and man-in-the-middle attacks can be pretty straightforward if some basic information or a few nodes of the system are exposed.

Industrial wireless sensor networks (WSNs) [260] have been considered as one of the pillars of enabling the transition from the old-fashioned wired industrial systems toward self-healing and controlling, flexible, and intelligent wireless control systems. Several standardized techniques for enabling industrial WSNs are discussed in [260]. These include ZigBee, Wireless HART, ultra-wideband (UWB), 6LoWPAN, ISA100, and blacktooth and blacktooth Low Energy (BLE) techniques. However, ISA 100 is the most commonly accepted standardized technique. In the ISA 100 standard, most of the security functions are optional, leaving room for security vulnerabilities. On the challenges of Wireless HART [261], authors in [262] explain that implementing security in the software of embedded devices will consume its processing, so much so that the devices will not be able to meet the 10 ms time-slots requirements of Wireless HART. Hardware accelerators are proposed, in such cases, to meet the processing requirements of security functions such as encryption techniques.

2) POTENTIAL SECURITY SOLUTIONS

Due to its massive role in InX, the security of IIoT requires several layers of security from strengthening the security of the device through software and hardware-based security hardening to operations security and minimizing its impact in case of breaches. Hence, the first step is to minimize inhere vulnerability levels of IIoT devices and then enforce and increase access control security on physical and logical levels on the critical infrastructures. Means to improve the security of the overall InX ecosystem include [34]: hardening IIoT devices against physical and tampering attacks, addressing communication-related weaknesses such as a lack of cryptographic techniques, and reducing the potential impacts of such weaknesses by identifying dependencies and increasing segmentation.

Since IIoT will leverage 5G technologies for connectivity the security solutions used for 5G will provide a good level of security for IIoT communications as discussed in [22]. Furthermore, authors in [263] discuss the use of blockchain [264], [265] and edge computing to secure the use of IoT in Industry 4.0. Blockchain, as discussed in [180], can enable trusted data sharing in a decentralized system comprising many edge nodes. Such frameworks, on the one hand, can meet the requirements of latency using MECs, and ensure security using blockchain, on the other hand. Security solutions for IoT from the perspectives of physical, medium access control, network, and applications layers are surveyed in [266]. Different architectural alternatives have been considered [267] for securing IoT, including distributed security with blockchains, as well as the use of fog and edge computing for data analysis, response, and secure storage-

The inherent limitations of IIoT that cause major challenges, i.e., resource limitations, can be overcome by utilizing the latest developments in other technologies, such as the extension of cloud platforms into MECs. The main purpose of MEC is to bring computation and storage resources into environments that need them, and SDN can be used to program the network at run-time to redirect traffic to such resources. Decentralized fog-based secure approaches [268] that use localized processing are proposed for the security of IoT in critical environments. Virtualization technologies can be used to slice resources into isolated domains even in smaller platforms such as MEC for isolation-based security. Furthermore, security systems that can be implemented with a low budget in terms of resources are highly important for IIoT. Therefore, methodologies such as header compression to enable encryption techniques on IoT devices that are capable only of low packet sizes or data rates can be useful [34].

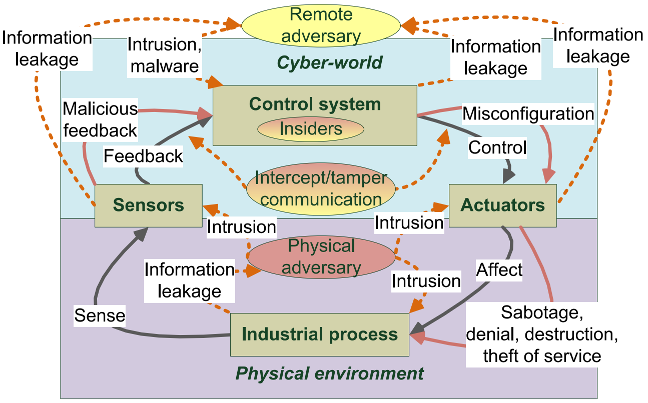

FIGURE 6. Security threats in cyber-physical systems.

One of the important methods of ensuring the timely availability of data in critical systems, specifically in industrial mixed-criticality, is to prioritize and de-prioritize traffic according to the delay sensitivity, reliability, or the criticality of the system, and service or the data. Data can be generally classified into safety, monitoring, and control [24]. Ensuring data delivery in industrial WSNs for critical systems with strict latency requirements through novel priority-aware data flow mechanisms is demonstrated in [9]. A plastic extrusion-based process monitoring scenario is used to define the protocol requirements and working principle of the proposed method. The protocol schedules access to channels for each data flow using a distributed prioritized medium access mechanism to guarantee channel access for the most critical traffic over others.

B. CYBER-PHYSICAL SYSTEMS

CPS can be realized with alternative connectivity mechanisms and support of different application protocols. CPS connectivity can be based on 5G and cellular networks, IP-based connectivity, or other wireless communication means, including, e.g., WiFi, blacktooth, ZigBee, as well as in distributed cases satellite, and LoRaWAN. On top of wired and wireless connectivity alternatives, lay different application-specific protocols, such as Modbus and Distributed Network Protocol (DNP3) for ICS as SCADA; IEC 61850 for smart grids; as well as controller area network (CAN), vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) protocols for vehicles. Therefore, CPSs also have security challenges and threats that migrate from these technologies, as described below.

1) SECURITY CHALLENGES

The main threats and attack vectors both from the cyber and physical world against CPSs are illustrated in Fig. 6. Central CPS elements – control system, sensors, and actuators, as well as physical processes – are organized into a feedback control loop and presented in Fig. 6 with brown rectangles. Physical, cyber, and cyber-physical attack paths are illustrated with red, yellow, and yellow-red ovals. Remote cyber adversaries may reach CPS systems, e.g., through management and control interfaces or software updates. CPS with Internet connections will face the remote cyber-threats of Industrial IoT as discussed before, in Section V-A. All CPS systems face threats originating from local connectivity, insiders, and the physical environment. Threats trying to compromise – tamper or disclose – sensing and control interactions. Physical threats against sensors and actuators as well as indirectly against the whole cyber-physical system are consequences of harsh environmental conditions or hostile adversaries within the weakly guarded industrial sites. The integrity of the control, sensor, and actuator platforms and software is threatened both by the cyber and physical world. Integrity and accuracy of the information collected from the physical world affect to the situational awareness and decisions made in the cyber-world. Control systems are increasingly utilizing big data and machine learning technologies, and are thus vulnerable to malicious or tampered feedback, adversarial learning [269], and other challenges, as discussed in Sections V-D and V-E. Consequently, physical-world attacks can escalate to malicious or misguided actions in the cyber-world, which then may cause even more damages – sabotage, denial of operation, destruction of physical devices, and thefts of service - in the physical processes.

The convergence of critical infrastructure cybersecurity and ICS takes vital significance in the context of InX. Critical process monitoring and control are crucial to InX's transformation of industrial operations through data-driven processes and innovative technologies. To this end, ICS plays a major role. On the other hand, due to the increased digitalization and interconnection that come with InX, cyber attacks might interfere with the operation of critical infrastructure by exposing ICS components [270]. This demands a thorough strategy to protect ICS and, consequently, the larger critical infrastructure that underpins InX. A foundational layer of security for InX is formed by safeguarding ICS against vulnerabilities, cyberattacks, and nation-state threats, as well as by strictly adhering to cybersecurity regulations. This ensures InX's resilience, incident response readiness, and public-private collaboration in the face of constantly changing cyber threats.

Current challenges include heterogeneity of devices and solutions, trust issues, as well as a lack of technical capabilities of devices used in industrial domains. The heterogeneity – different applications, various types of devices, and protocols – means that the security standards and solutions are fragmented. This causes technical interoperability issues and increases the complexity of the security architecture. CPS can be based on different connectivity and application alternatives. These alternatives have their security protocols for assuring the confidentiality and authenticity of the communication. Application-specific protocols either integrate their security approaches or rely on the underlying communication security. A challenge in the past has been an assumption that CPS are closed systems and operated in a trusted physical environment [26]. This leads to solutions that are non-secure-by-design.

Securing the whole life cycle of CPS components is also a challenge. In addition to technical protection during the operational time, supply chains must be verified. Components should be assured or trusted not to contain hidden vulnerabilities and to provide the required security level. In complex industrial settings, the security of supply chain management depends on several factors and suppliers, and the amount of involved persons increases the risk of insider attacks; the supply chains are dynamic and constantly changing, and the liabilities may also be unclear due to lacking legislation. Managing trust as well as finding supplier-specific problems and vulnerabilities can become a complex challenge [271].

2) POTENTIAL SECURITY SOLUTIONS

CPS security relies on confidentiality, authenticity, and access control functions that are provided by a) connectivity mechanisms [27], b) physical layer [170], c) end-to-end protocols for CPS applications [171], as well as d) platform and interface controls of controllers, sensors, and actuators [163]. Security architecture for addressing known threats against CPS systems is facilitated by recommendations and best practice documentation that have been produced by industrial cooperation. For instance, ENISA has produced guidelines for securing software and development life cycles [272]. Further, cyber ranges [179] are emerging to facilitate isolated security testing of CPS. Security metrics have been defined [178] to facilitate holistic security analysis and design of industrial CPS.

CPS is characterized by feedback loops. While these loops for control are applied for various industrial applications, they can also provide reactive security protection for CPS. Different anomaly detection and machine learning approaches [172], [173], [174], [175] have been proposed for CPS to enable detection and reactions to intrusions, malware, anomalies, and other threats. Solutions for making the control systems robust against malicious or tampered feedback data include teaching machine learning to be resistant or to detect adversarial samples [273], [274], [275], [276].

Solutions addressing the security challenges arising from heterogeneity [176] in the application or the connectivity layer can be divided into two main categories: through a common language, which is achieved with standards [277] or semantic approaches [278], or through mediating middleboxes, such as gateways or proxies. Solutions for industrial communication network security are in general applicable to industrial applications of CPS. Technology and process-related aspects and requirements for industrial cybersecurity have been specified and standardized, e.g., in IEC

62443 [164], [277], which provides a risk-based framework for managing the security of industrial actors.

In ICS, the problem of sophisticated industrial attacks is addressed by NeuPot [279], an ICS honeypot technique based on neural networks. Using a time-series forecast model and a Modbus honeypot framework, it improves security through better honeypot interaction and cyber threat detection, showcasing exceptional efficacy in both areas. The objective of the research presented in [280] is to identify off-path false-data-injection attackers in ICS while they are in their hiding phase. Using secret keys, the defense approach described in [280] continually introduces tiny distortions into sensor data to ensure accurate and timely identification of hidden intruders without interfering with regular ICS operations. A compromise between control performance and detection efficacy is taken into account by the ideal design of ICS watermarking, which was implemented in [281]. Here, the technique uses an optimization strategy to estimate the watermark strength, and updates detection metrics to lessen the impact of noise. Both theoretical analysis and real-world trials show the method's higher performance.

Heterogeneity introduces the need for additional solutions and hence complicates systems, which in turn may enable new vulnerabilities. These vulnerabilities from complexity can be managed by isolating different applications and technologies from each other. Due to the existence of different kinds of systems and devices with different security capabilities and risks, systems are commonly [277], [282] divided into zones or segments with different security levels to isolate security breaches and attacks. Network solutions for segregating different CPS processes have leveraged learning-assisted network slicing [165] where different applications are automatically recognized and isolated. However, in the end, complexity and security challenges must be solved separately using approaches that are suitable for the applied technologies and physical process, e.g., with power-grid [166], power-plant [167], charging station [168], or autonomous vehicle [169] – specific cyber-controls.

C. ADVANCE ROBOTICS

Robots have unique characteristics regarding data collection, learning, mobility, and decision-making, they are mainly built through the interconnection of a wide variety of components such as sensors, communication devices, and actuators, mostly interconnected by a wireless network. Since robots were originally designed to be part of isolated systems, security was not an integral part of their design, resulting in trivial OS-related, protocol-related, as well as hardware-related threats. With the advent of Industry 4.0, paradigms like cloud robotics, and the almost ubiquitous presence of robot systems, copious amounts of data produced by plants need to be analyzed and sent over communication networks to remote servers for further processing. Given the pivotal role of robot systems in InX, security in robotics has a top priority due to the impact of their vulnerabilities in the chain of production [283].

1) SECURITY CHALLENGES

Software found on robot systems is usually outdated and relies on weak or even obsolete cryptographic packages. This issue is as relevant for robots as it is for computers, software will no longer receive security updates which increases the possibility that vulnerabilities become popular among attackers. Since novel security mechanisms are not present, the impact of software vulnerabilities radically increases, improving the success probability of an attacker, and hindering any detection efforts [181]. Another important threat is the lack of security mechanisms in the protocols used for robotic systems, as they do not integrate authentication or integrity methods to detect suspicious behaviors.

The Robot Operating System (ROS) is a popular development platform for robotics that uses a publish/subscribe model, from a security point of view this model is insecure as publishers cannot verify their data, and subscribers can't verify the data received. The lack of encryption, and therefore privacy, increases the risk of attacks like man-in-the-middle as well as hijacking. Man-in-the-middle refers to an attack in which a malicious node acts as a relay and can alter the communications between two parties who are unaware of the situation [284]. A hijacking attack occurs when a malicious node assumes control of a session between a server and a client and replaces the incoming packets with new packets that are sent toward the destination [285]. In the same manner, the use of outdated cryptographic libraries is not beneficial, as is misconfigured cryptographic software such as shared, symmetric keys for virtual private networks (VPNs) [286], [287].

Without proper measures for confidentiality, integrity, and privacy, attackers can eavesdrop on published data and modify messages, altering the robot's behavior. More specifically, an attacker can access and modify the configuration parameters of robots, alter the logic of the program being executed, change the commands being sent by a remote operator, or inject false information regarding the robot's status. Damages caused by the mentioned attacks vary from defective products to operator injuries [182]. ROS architectures allow clients to initiate remote communication with a robot via its IP address, this is necessary for use cases such as remote operation, or video streaming from a robot's camera. Such exposure causes a massive vulnerability as found in [83], where a considerable amount of master ROS nodes were listening on port number 11311, leaving the robot systems behind them vulnerable to malicious users. Robots are also susceptible to physical attacks, like the use of their USB port for executing malicious commands, or the connection to a robot's controller using the RJ-45 port from which the attacker can access other system components [288].

2) POTENTIAL SECURITY SOLUTIONS

It is of vital importance to avoid robot systems running on outdated software, the best method to achieve this is by regular updates and upgrades. While some software often updates in the background, this is not always the case, the principal practice is to look for available updates and if available, install them. The purpose of updates is to provide general maintenance to software, as well as install patches against vulnerabilities and improve threat protection [183]. Similarly, upgrades are needed to keep software healthy, they usually introduce considerable changes and might not be needed right away. Nevertheless, vendors eventually stop supplying updates to old software, and in such a case upgrades are necessary to avoid running outdated software [289].

Protocol security can be improved by adopting one of the available robot application frameworks, although the security level offered varies depending on their popularity and scope. Data Distribution Service (DDS) is a connectivity framework for distributed systems capable of performing authentication and encryption for remote client discovery via Real-Time Publish-Subscribe protocol (RTPS) packets that run over any transport [290]. DDS also offers support for Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS), besides authentication and encryption DDS is also able to implement access control, data tagging, and security events logging [291]. The Internet Communications Engine (ICE) is an object-oriented framework that provides encrypted bidirectional connection and supports SSL at the transport layer. Although SSL has been rendered as too heavy for constraint devices, there are lightweight implementations available for embedded applications [292].

The most popular solution is the already introduced ROS, which is developed under a publish-subscribe approach. ROS includes its communication middleware, but unfortunately, it does not provide security features by default, except for client isolation in Virtual Private Networks (VPNs). However, due to its wide adoption, ROS has been enriched with several extra features that significantly improve its security capabilities. Research has contributed by adding security features to ROS, such as the use of Web tokens for secure authentication of remote clients [291], [292], [293], and the use of cryptographic methods to ensure data confidentiality and integrity as well as the use of an authentication server to certify only valid clients form part of the developed application [185]. SROS is another extension aimed at providing ROS with modern cryptography and security capabilities, enhancing security at transport encryption, access control, and process profiles [184], [294].

D. BIG DATA ANALYTICS

Security in the realm of big data will be multi-pronged. For example, avoiding errors in the data and its analytics will be of paramount importance due to the criticality of the decisions based on the data or analytics. Thus the data must be protected from errors as well. For example, in InX, there will be large, diverse, structured, or unstructured data produced by smart sensors, devices, log files, and video and audio in real-time. There will also be decisions based on the data. Security verification before making critical decisions based on such data will be extremely important. Security of hidden patterns and unknown information extracted from big data is essential for better decision-making, preventing situations of uncertainty, and mitigating the possibilities of malicious activities. Below, we discuss the most important security challenges that are linked to big data in the realm of InX.

1) SECURITY CHALLENGES

The developments in the management of high-stream industrial data in InX ecosystems bring numerous technical challenges. Data will be generated by an overwhelming amount in InX. Technology has advanced to the extent that hackers can access the data to extract vital information. For example, unauthorized data transmission across different unauthenticated groups in InX can lead to data leakages and it imparts potential risks to industrial data that need care and security [295], [296]. In addition, the lack of proper authorization techniques can result in data breaches, which can be an extremely serious concern in InX, resulting in access and stealth of sensitive data [297]. False data injection, as discussed in [298] is another challenge, through which most of the functional, as well as non-functional requirements of data-driven applications in InX, can be in jeopardy. The reliability in the transmission and reception of IIoT data is also a serious concern. Industrial data acquired from IIoT devices in InX applications, as discussed in Section V-A, is prone to corruption attacks unless treated with robust big data analytic engines and appropriate encryption schemes [101].

Learning-based frameworks used for InX applications, associated with industrial big data, demand rigorous training of the data. Such frameworks consume huge computational resources, as well as require robust learning models. Furthermore, the training models used for data analytics are also subject to security threats and the data could be anonymized by hackers [299]. Such learning-based frameworks in InX applications are prone to cyber-attacks. The ultimate aim of such threats includes false decision-making. Moreover, data spaces in the context of InX are virtual environments that are essential to securely organizing and sharing data. Centralized data spaces can be prone to DoS or similar attacks, resulting in vulnerabilities like single-point-of-failures or restricting availability. Such threat necessitate serious efforts in terms of solutions, which are described below.

2) POTENTIAL SECURITY SOLUTIONS

There are many use cases of InX in which big-data analytics have already been used. The most promising solution for avoiding security breaches and data leakages is developed by Xu et al. [139] using a blockchain-based framework integrated with watermarks. Here, InX use cases can be used to selectively exchange data with other blockchains, which are accountable for resisting information leakage. Injection of hardware trojans on industrial data also suppresses the data breach threat and avoids data leakages [300]. Such techniques implement Trojan triggers using capacitors and are tested under different operating conditions. Trojan trigger accounts for securing the big data in InX applications from leakage vulnerabilities. Integration of IoT-based frameworks could help monitor and control the cyber security attacks on industrial data [140]. Security aspects of IIoT systems in InX applications could be carried out by incorporating appropriate security and encryption with the support of blockchains [301], which provide secure and trustworthy services. Also, the usage of dual dynamic key [302], and lightweight searchable encryption protocols [303] enhances the reliability in the transmission of IIoT data.

The role of learning-based techniques is crucial in industrial big data analytics, particularly for anomaly detection on data [142]. Some of the machine learning techniques such as SVM and Random forests are used to provide anomaly detection [143] using real-time industrial data [141]. Wang et al. [304], propose an approach of using feedback on big data and coordinating the behavior of intelligent agents for secure decision-making in smart industries. This approach self-organizes the agents driven through big data for autonomous decision-making and provides strategies for deadlock prevention and intruder avoidance through proper negotiation mechanisms.

Autonomous inventory management is one of the crucial operational tasks in smart industries. The authors in [305], deployed UAVs as autonomous navigating agents for automating inventory tasks by processing the big data collected by UAVs. It was also integrated with a blockchain architecture for ensuring security and transparency. The system is also capable of managing external audits using big data analytics. Since cloud systems and extensions of clouds such as edge and fog computing will be crucial for InX, and the security of most of the big data will be directly affected by the security of cloud platforms, in the following subsection, the security of cloud computing platforms in the context of InX is discussed.

In the context of data spaces, decentralized data sharing, in which data is dispersed throughout a network of nodes, rather than kept in a single repository, is essential [306]. This decentralization lowers the possibility of a single point of failure while improving data security. Interoperability is given top priority in dataspace technology, enabling smooth communication across various data sources, formats, and protocols. It preserves data sovereignty, guaranteeing that businesses maintain authority over their data and abide by privacy laws. Robust security protocols, data governance, scalability, and real-time access are essential components that facilitate data-driven decision-making and streamline operations.

E. MACHINE LEARNING

Machine learning has been widely researched and used for improving the security of communication systems [123]. Due to the increasing volumes of data traffic, machine learning has been an important field of research specifically in terms of security, since human monitoring is rendered useless in traffic analysis. Since the learning systems are external to the systems of InX, such as CPS or IIoT systems, there are chances of security lapses and vulnerabilities without having the devices compromised. This is important in cases of strong isolated industrial domains that use machine learning. Therefore, the security of machine learning in the context of InX is even more important due to the critical nature of the infrastructure, as well as the dependence of many systems of InX on machine learning. Below, we discuss some of the most pertinent challenges and potential solutions.

1) SECURITY CHALLENGES

Even though it is security-hardened, some of the properties of machine learning can induce basic vulnerabilities in the systems machine learning operates. Several security challenges of machine learning are described in [78], mainly concerning 5G. However, the threats can persist in InX. For example, one of the main threats that machine learning can induce in the systems is the denial of detection (DoD). The DoD can prevent machine learning from generating signals, for instance, from events, failures, and even cyber-attacks using adversarial examples [307] and data poisoning [308]. Another threat that machine learning can induce is leaking sensitive information from the company or factory. These attacks will be very critical in InX. The components of InX need to be constantly monitored and numerous signals for a vast number of functions and services will be created. The blocking of such signals, for instance with DoD, can have serious consequences in many stages such as processing and specific maintenance. Similarly, if a machine learning algorithm shares data with a malignant entity, the security of InX can be compromised. On top of such weaknesses within machine learning systems, the concepts of adversarial machine learning [309] that attempt to fool machine learning models are worrying. For example, the model poisoning attack shown in [310] for federated learning can have huge consequences in InX.

By leveraging distributed learning, traditional fog computing is evolving toward edge intelligence. The security challenges of introducing deep learning in fog computing mainly include model fairness [311], adversarial robustness [307], [312] and privacy-preserving [146], [313]. Attacks on such edge intelligence frameworks refer to those that mislead the deep learning models using poisoned data (e.g., adversarial examples) and those that compromise the original inputs of pre-trained learning models using any publicly accessible information (e.g., gradients, open datasets, and development tools) that is not very privacy-sensitive. Meanwhile, with the rapid deployment and increment of deep learning-based intelligent infrastructures, users can have the possibility to join/access the edge intelligence as a service (EIaaS) platform and share their learning services. In such cases, attacks can happen in edge intelligence architecture by providing uncertified data and learning parameters.

2) POTENTIAL SECURITY SOLUTIONS

To deal with these challenges of machine learning in InX, trustworthy machine learning techniques have drawn much attention [314]. Different from environmental modelling [315], such as reinforcement learning, supervised learning, and unsupervised learning, trustworthy machine learning is investigated to improve AI's privacy, security, and interpreter-ability. For InX, potential application scenarios of machine learning include industrial unmanned systems, industrial data analysis, quality detection, etc. Due to its importance in the critical infrastructures of InX or industrial society, adversarial threats on machine learning should be studied first to identify hidden attack surfaces. Nowadays, known threats including adversarial examples as highlighted in [316], such as data poisoning, backdoor, and membership attacks have been widely studied, and many defence strategies have been implemented.

According to the types of adversarial threats, promising defences can be divided into four parts: 1) defending against adversarial examples; 2) defending against data construction, and 3) defending against backdoor attacks. Each part also contains several sub-branches. For adversarial examples, the most popular defence methods are adversarial training [317], and differential privacy [318]. However, adversarial training often needs more data samples and the added noises of differential privacy are harmful to model accuracy. To enable black-box defence against the adversarial example of industrial malware classifiers, authors in [319] designed a stateful query analysis method and a novel distance metric to improve the threat hunting rate. Besides, a conditional generative adversarial network is proposed in [307], which also can be used to identify the adversarial example of industrial vision applications in a black-box way without reducing model accuracy. For data poisoning attacks, there are three different defence parameters, including poisoned data detection [320], abnormal feature detection [321], and back door model parameter detection [322]. The challenges of preserving data privacy in machine learning to maintain company information or factory floor plans can be addressed with privacy-preserving federated learning approaches, such as discussed in [147].

VI. SECURITY OF INDUSTRIAL APPLICATIONS

InX will have an enormous number of applications, mostly of critical nature dealing with critical infrastructure and information. Therefore, its security will be extremely important. In this section, the security of two main application areas in the realm of InX is discussed.

A. INDUSTRIAL AUGMENTED REALITY

Industrial augmented reality (IAR) applications incorporate tele-presence systems in which a person can guide an operator, a person or a robot, remotely to reduce the need of physical movements in factory environments [129], [323]. IAR has been used in extremely sensitive operations to help operators in complex environments, for example, inspection in the aviation industry, as discussed in [324]. IAR also plays an important role in mirroring the physical world, such as the factory environment, in a digital one, which will be vital for InX [325]. Therefore, its security is also very sensitive and must be ensured. In a conventional AR architecture, an AR handheld mobile or head-mounted device is the main entity, which can be controlled by smartphones, tablets, or special AR glasses like Microsoft HoloLens. An AR application takes input data from the camera of the device, stores it, and/or sends it to a remote server. This data is then transformed into virtual objects, which renders the data and overlay output directly on the user's perception in the real world [29], [326]. Since IAR systems require tactile interaction with users, the IAR system need to exchange and manage content as fast as possible and needs to manage a large amount of data. The communication between IAR devices is wireless and expected to enable dynamic on-demand information sharing, which requires a fast response from the remote servers [327]. Modern communication architecture/technologies, such as fog edge computing, and cloudlets, extend support to IAR applications. Edge computing helps meet the real-time requirements of AR and reduces the dependence on uninterrupted high-performance communication channels to the computing servers [85]. The advent of 5G brings high bandwidth and low latency to enable users to achieve high-fidelity telepresence systems and collaborative augmented reality applications [40]. Since IAR involves many 5G-based technologies and comprises IoT devices (head-mounted displays [328]), it will incorporate the security challenges of these technologies, as well as have its security challenges, as discussed below.

1) SECURITY CHALLENGES

The challenges of IAR are multi-dimensional, including those existing in IoT devices (IAR devices), those arising from the communication infrastructure (e.g., 5G), and those related to storage of the sensitive data. Many risks are associated with the input data, as data is coming from various sensors which are always on such as cameras, GPS data, temperature, accelerometer readings, and more. The confidentiality, integrity, and availability of this data need to be ensured because an attacker can distill sensitive data like passwords, and secret formulas, among other private matters from the visual information. Continuous sensing and video streaming may not be sensitive to the user but may be used by others, such as bystanders resulting in bystander privacy leakage [29], [329].

There are also risks involved with the output of AR, such as the capability to modify a user's view of the environment. AR content may include static data that consists of non-sensitive data like product images, and tutorials, and sensitive data, such as computer-aided design (CAD) models which must be protected. A malicious or buggy application may potentially obscure the real-world information or occlude virtual content of other applications and may cause other attacks like clickjacking [29], [329]. One result of such a security attack can be to show the wrong speed limit instead of a real speed limit. Another case can be to cause a sensory overload of users by flashing bright lights on the display or delivering intense haptic feedback [29], [329].

As AR applications process and access data from various sensors, a big risk is involved in stealing the data or misusing that access. An attacker has a high interest in retrieving the processing/processed data, to try to manipulate the data to lead the machine operator to take wrong measures. Overall, this can cause process disruption or even technical and health damage, as discussed in [29], [85]. In IAR systems, a lot of collaboration is carried out using audio-video teleconferencing and computer-supported collaborative work (or CSCW). This enables the live sharing of information among multiple users, where interaction takes place in the same shared space physically or virtually, using shared space technologies. Using these shared spaces a component vendor can help a plant/machine operator to fix an error in a particular machine by embedding the instructions into the video stream without visiting the site/location [330]. Various threats arise in such shared spaces/technologies that include spoofing, and unauthorized access from personal area networks (PANs), such as in ZigBee or blacktooth PANs [329].

2) POTENTIAL SECURITY SOLUTIONS

The security assets of an IAR architecture need to have adequate mechanisms to protect the input data against eavesdropping, voice-spoofing, shoulder-surfing attacks, and manipulation [329]. Authorized and authenticated users should be able to access static and process data, and read access shall be possible [29]. Biometric authentication, such as voice recognition or facial recognition, provides attractive solutions for secure authentication and authorization. Khamis et al. [331], [332] proposed two multimodal schemes, called GazeTouchPass and GazeTouchPIN, that combine gaze and touch for shoulder-surfing resistant user authentication on mobile devices. These models require an attacker to simultaneously observe the device screen and the user's eyes to find a password, for example.

Looks Good To Me (LGTM) is an authentication protocol that uses a combination of facial recognition and wireless localization information to cross-authenticate users. In simple words, users can authenticate and initiate sharing using an AR head-mounted display (HMD) with a wireless connection [156]. HoloPair, however, avoids the use of wireless localization, which may be unavailable and inefficient in devices, and instead utilizes the exchange of visual cues between users to confirm the shared secret [154]. Lebeck et al. [333] has laid the foundation for the security of AR visual output and designed a prototype platform called Arya that implements the application output control based on the context-specific policies, and evaluated Arya on various simulated scenarios [329]. Ahn et al. [334] build upon Arya, a novel system for dynamic and complex environments to ensure integrity, availability, and confidentiality using reinforcement learning automatically [329]. Anonymization techniques, to obfuscate the location of users, can be used to secure location-based services in industrial contexts [335].

Biometrics is one of the ways of authenticating cloud computing architecture and has potential benefits. Benefits such as scalability, cost-effectiveness, reliability, hardware agnostic, and allowing ubiquitous access to private data and services. Biometric credentials have the advantage of not relying on the user's memory [336]. Another approach is using the local computing and storage enabled by Edge computing. Edge computing helps meet the real-time requirements of AR and reduces the dependence on uninterrupted high-performance communication channels to the computing servers. One approach for such services, in which a sensing device gathers sensitive data in an environment, is moving the service or techniques that use that sensitive data into the environment generating the sensitive data as discussed in [110].

B. BLOCKCHAIN

Blockchain improves the transparency of the overall processes, and therefore generates trust by revealing the potential flaws and misbehavior in the operation of different components and stakeholders, by keeping track/record of each phase in a particular industrial application. Moreover, blockchain would allow a zero-trust management mechanism [337], [338] for the InX applications that will regularly ensure each operation is carried out in a trustworthy manner. Zero-trust is a security model that assumes any person or device attempting to access a network is already compromised, which must be verified before access is granted. Blockchain can be used as an enabler for zero-trust by, e.g., eliminating the need for a central trusted authority, ensuring that data cannot be altered and that all nodes on the network agree on the validity of transactions, and providing a transparent and auditable ledger that can be used to track user or device activities in a zero-trust systems. Therefore, blockchain can fulfill the InX requirements by providing decentralized secure, trusted, and optimized solutions [339].

Blockchain technology provides a zero-trust computing environment for industrial applications through a shared distributed ledger that possesses all the transactions and each of the involved participants can monitor these transactions. Thus blockchain further improves the security of the whole value chain by ensuring data integrity, transparency, and trust. However, the current blockchain systems still suffer from some security threats, i.e., at the network level, in the smart contracts/agreements, and during transactions. In the following part, we discuss security challenges in blockchain in the context of InX.

1) SECURITY CHALLENGES

Generally, blockchain technology improves overall security and data breaches as it provides key features such as decentralization, distributed trust, immutability, and better data access control mechanisms. However, there are open challenges for data privacy, for example, because of the openness and transparency of transactions among various involved entities of the system. The work in [340] presents the need for careful assessment of the transparency and privacy of transactions through blockchain-based multi-hop tracking and tracing mechanisms. It also imposes a strong emphasis on information accountability, privacy in a dynamic environment, and real-world evaluation of blockchain frameworks for privacy preservation in industrial supply chains.

The use of blockchain technology for communication networks raises numerous security and privacy concerns in various smart applications. For example, potential threats from network perspectives of blockchain may include eclipse attacks, DDoS attacks, Sybil attacks, time-jacking attacks, and transaction malleability attacks, among others [94], [341]. The eclipse attack in the blockchain network can occur when an adversary wants to take control of incoming and outgoing traffic by isolating the IP addresses of the other/legitimate nodes through a victim node [162]. Though the blockchain network works/follows similarly to the peer-to-peer network, it still suffers from DDoS attacks which make the desirable resources unavailable [342]. The Sybil attack allows the hostile peer to dominate the whole network by creating several fake identities [158], [343]. In a time-jacking attack, the adversary tries to interrupt the mining process by inserting inaccurate timestamps [344]. Transaction malleability threats can result in an inconsistent state of blockchain and open doors for further attacks [345].

One of the popular threats known for the blockchain is the '51% attack', where a miner node or a group of miner nodes take control over more than 50% of the hashing rate/computing power of the network, which results will prevent the other miners to mine a new computing block [346]. In this case, the double-spending attack is quite certain as the transaction/data can be altered easily and that may lead to further challenges in the verification of new transactions [347]. In a selfish mining attack, a group of miners either want to increase revenue/reward by dominating the majority of the network or try to waste the resources for legitimate miners [348]. Furthermore, all the transactions in the blockchain systems are shared and traceable, which raises privacy risks as the adversaries can easily track the real identities of the involved entities [349]. Anonymity is required in the case when the sensitive data is shared over the network and any of such involved entities/stakeholders can track the traffic of the network.

The consensus algorithm in the blockchain is dedicated to verifying/validating the authenticity of each transaction, but it is still possible to target the authenticity of the transactions. The transaction authenticity in the blockchain is highly dependent on the cryptographic operations, i.e., each new transaction is connected with the previous one using digital signatures/cryptographic schemes [350]. The attacker can perform double-spending by delaying or denying the delivery message of the new transaction. Blockchain technology also faces several obstacles due to the vulnerabilities in smart contracts. For example, there are about 12 different kinds of vulnerabilities in the smart contract identified in [351]. Some of the most common attacks include re-entrance vulnerability, coding errors, and timestamp dependence [263]. These types of threats are likely to occur both in the Ethereum Virtual Machine (EVM) and Solidity (programming language).

2) POTENTIAL SECURITY SOLUTIONS

There are different solutions for addressing different types of security challenges in blockchain. For example, in addressing the network-related threats of blockchain, specific approaches are proposed in the scientific literature. The challenge of eclipse attack can be countered by proposing an anomaly detection system (ADS), and by introducing randomness [162], [160], [161]. Distributed IDS mechanisms, game-theory approaches, and proof of activity protocols can be considered to address DDoS challenges in the blockchain [352]. Sybil attacks can be resolved by developing secure consensus mechanisms [157], and by distributed behavior monitoring of miner nodes [158]. To overcome the time-jacking threats, synchronized clocking techniques must be placed during the blockchain transactions [353]. Transaction malleability attacks can be eliminated using the provenance-based scheme, i.e., provide an extra layer of the provenance [354].

Threats, such as '51% attack', double-spending, and selfish mining are not very straightforward to launch because they require higher computing power. The '51% related attacks' can be countered by two-phase proof-of-work" (2P-PoW) [355], Random mining group selection approach [356], and Proof of Activity protocol [357], [358]. The potential countermeasures to the double-spending attacks can be the non-interactive zero-knowledge (NIZK) proof, increasing confirmation, and deep inspection/listening/observing [359]. Several approaches such as the "truth state" strategy [360], the Freshness Preferred (FP) strategy [361], and ZeroBlock [362] scheme can be practiced to avoid any of such selfish mining threats, [363]. To ensure privacy protection in the blockchain systems, some of the potential solutions such as homomorphic encryption technology and zero-knowledge proof can be adopted [159]. Furthermore, the concept of off-chains (which was originally proposed to improve the scalability of the blockchain systems) can play a key role in the confidentiality of the information.

Blockchain-based decentralized data integrity, security, and trust schemes for Industry 4.0 have been proposed in [180]. The proposed framework, called BlockEdge (integration of the blockchain and edge computing), provides the necessary levels of security within the resource constraints and latency limitations. Also, the research work in [263] identified potential security challenges and solutions for blockchain-edge integrated communication networks.

Various solutions addressing the smart contract-related vulnerabilities are presented in [364], [365]. Moreover, authors in [366] classified the smart contract attacks into four categories (i.e., malicious acts, weak protocol, defraud, and application bugs), and also presented the attack techniques as well as the relevant security approaches.

VII. RISK MANAGEMENT AND SECURITY STANDARDIZATION

InX requires proper risk management to assess the security of the overall ecosystem and related consequences. The security of the InX ecosystem also needs agreements between different stakeholders to maintain the best security policies and approaches. Risk management and standardization play crucial roles in this regard. There are also challenges, such as fragmentation in standardization related to IIoT [367], which need to be solved through proper security policies on the organizational level if standardization fails or introduces delays in applying the best practices. Evaluations from other than standardization bodies can also be followed. For example, security recommendations for threats and vulnerabilities in ICSs, including automation, process control, and I&C systems, are published regularly by the German Federal Office for information security [368]. These include the latest top threats, countermeasures, or solutions for those threats and the existing gaps. Similarly, the National Institute of Standards and Technology (NIST) [369] provides a framework for improving the security of critical infrastructure [370]. The framework applies to ICSs, CPS, and the IoT, which deploys a risk-based approach for managing cyber security risks. Such recommendations must be followed besides the specific efforts from standardization bodies. Below we discuss risk management and standardization efforts in this regard.

A. RISK MANAGEMENT

The diverse technological issues of InX emphasize the heterogeneous and dynamic nature of contemporary cybersecurity. Cybernetics, as a discipline of control and communication structures in technical and social systems, helps in approaching cybersecurity risk management. Accordingly, when managers organize factories or supply chains, they face increasingly complex situations and problems of how to make optimal decisions [371], [372], [373]. The diverse approaches in cybersecurity risk management include incident response and proactive approaches to preventing and preparing. However, whatever organizations' actions in terms of technical progress, contribute to the growth of complexity, making any future response more demanding and urgent. To keep up with the development of possibilities, resources, technologies, etc., we can talk of an arms race [374].

In the specific context of industrial environments, cybersecurity also has an impact on system safety. It is a relatively recent observation that the two aspects, though traditionally treated separately, are interdependent and must be considered jointly [17]. An additional implication for cybersecurity risk management is that any technical system is only temporarily secure and that cybersecurity should be seen as a continuous activity [374]. The way forward will be about building resilience in production systems and supply chains. This includes considering resilience already in the design phase of new structures, developing effective metrics that can help evaluate vulnerability and resilience, and simulating complex industrial systems to understand vulnerability issues better [375], [376]. An important aspect will be to automate safety and security risk assessment and extend it from design and engineering time to the regular operation of production systems [377].

There should be clear organizational policies regarding security policies, methods for implementing those policies, and training of the staff to work securely and maintain the security of the systems and components of InX. Insufficient policies and lack of knowledge of the staff result not only in direct security threats but also in the propagation of security threats through unintended facilitation for subsequent attacks. This underscores the need for zero-trust-type system approaches. Lack of sufficient security knowledge of the staff can impede the detection of threats, recovery from threats, and sanitizing processes. One of the most prominent security policies concerns the use of external applications, as discussed in the recommendation by the Federal Office for Information Security of Germany [378]. Proper monitoring for external applications and internal applications with write capabilities must be ensured. Such applications operating in insecure environments, for instance, can induce security vulnerabilities. Policies for lost devices, passwords, the use of personal/private devices, trust establishment techniques, as well as methods for stopping insider attacks, must be devised at the organizational level.

B. STANDARDIZATION EFFORTS

Security of industrial systems has been the focus of several standardization organizations that are either positioned at generic information technology - computer science level or are domain specific, as summarized in Table 4. NIST has produced a series of information security guidelines and standards, where the flagship document is a collection of special publications on managing information security risks [379]. These publications present the basic principles at an organizational level for assessing, responding to, and monitoring risk. IEC has published the IEC 62443 series of standards on the security of industrial networks and communication systems [380]. The IEC approach focuses on the prevention and management of security risks. These standards introduce some fundamental concepts like process maturity levels, security levels for systems, defense in depth, and the division of the system into zones and conduits. The standard offers architecture reference models, system partition models, as well as relationships among models for security management. Also, IEC 62443 recommends

TABLE 4. Relevant Standardization bodies and their activities.

Technology	Standardization Organization	Standards, Deliverables, TRs, Recommendations	Description
5G	3GPP	3GPP TS 33.X, TR 23.700-20, 3GPP TS 23.501, TSG-SA WG2, FS-IIoT	3GPP covers security aspects from the 5G network and vertical aspects of the 5G, mainly under S3. There are also various groups under the auspices of 3GGP, such as 5G-ACIA that covers security of IIoT, etc.
	ETSI	ETSI EN 303 645,	ETSI standards can help deploy private networks in InX, for instance through MEC
	ITU	ITU-T-X.509, ITU-T X.805, ITU-T X.1215, ITU-T X.1361, ITU-T X.1500	Recommendations for security, ranging from security of telecommunications systems and architectures to users of ICT.
CPS	3GPP	3GPP TS 22.104 v16.0.0.	Covers the CPS aspects in conjunction with 5G as the connectivity infrastructure to protect industrial data from manipulation.
	IEC	IEC 62443, ISO/IEC 15408	Risk-based framework for industrial security and the ”Common Criteria” framework for security requirement specification and evaluation.
	CPSSEP	JA7496, JA7496A	Ensure security practices and manage risk issues in CPS.
IIoT	CESMII	RRI	Incorporates robots and energy-efficient smart manufacturing
	IIC	IINF	Put forwarded safety standards from a security perspective
	IISF	IEC 62443	Establishes best security practices.
	IEC	IEC 61443-4-1, 62443-4-2, ICSA	IIoT integrated industrial control and IIoT Component Security Assurance.
Big Data Analytics	ISO/IEC	ISO/IEC 20547-4:2020	Provides reference architecture for big data with simplicity for ensuring overall security.
	ETSI	ETSI GR SAI 002	Data supply-chain security for AI
	IEEE	IEEE 2813-2020	Big data business security risk assessment to assess business security risk control through the big data technology
Machine Learning	IEC	IEC-5259	Ensuring data quality for analytics through ML
	NIST	SP 800-94	Guide to Intrusion Detection and Prevention Systems (IDPS)
	3GPP	TR 23.700-80, SP-211443	3GPP since release 18 has started covering AI and ML for networks and verticals, including its security aspects.
Cloud Computing	DMTF, SNIA,	SPDM 1.2.0	Helps to use standardized platforms through security protocols.
	ETSI	EN 303 645	Prevents large-scale attacks against smart devices.
	OASIS	ebMS 3.0	Defines a secure and reliable exchange of data.
Advance Robotics	IEEE RAS	RAS/SC 7007	Presents a set of ontologies that represent norms and ethical principles; data privacy and protection; transparency and accountability
	ANSI	ANSI/RIA R15.06-2012, RIA TR R15.706-2019, ASTM E2855-12(2021)	Provides the main safety measures as well as secure M2M communications between robots.
UAVs	ISO	ISO 14508	Specification for system security for UAS
	ASTM	ASTM F3411-22a	Standard Specification for Remote ID and Tracking for UAS
	3GPP/ETSI	TS 33.256, TS 23.256	Security, connectivity, identification and tracking aspects of Uncrewed Aerial Systems (UAS)
Augmented Reality	IEEE	IEEE P2048.4, IEEE P2048.5	Person identity and environment safety standards for VR and AR.
	XRSI	Privacy and Safety framework version 1.0	Technical, physical, administrative, safety and privacy standards, framework and guidelines in XR
Blockchain	ISO	ISO/TR 23244	Focus on privacy and personally identifiable information protection.
	ASC X9	ASC X9 TR 54-2021	Set of quality management standards with distributed environmentally sustainable ingredients.
	ERC	ERC 1400, ERC-3643	Smart contract standards that manage compliance by leveraging the security tokens.

requirements for security such as access control, data confidentiality, limited data flow, resource availability, identity identification, and authorization, among others. These security requirements enable three different security levels, target security levels (SL-T), achieved security levels (SL-A), and capability security levels (SL-C).

The ISO/IEC 15408 is a three-part standard [381] that defines a set of requirements for designing security functions, as well as for security assurance and evaluation. ISO/IEC has also produced the 27000 series of standards (27001,2,3,4,5) [382] on information technology security techniques with a broad scope covering technical cybersecurity, as well as privacy and confidentiality topics. Apart from generic standards, domain-specific standards provide more detailed and focused guidance. As an example in the heavily regulated nuclear energy domain, IAEA has published a technical guidance reference manual within the nuclear security series [383]. Similarly, IEC 62645 [384] presents nuclear Instrumentation and Control cybersecurity requirements and IEC 63096 [385] includes security controls that are applicable in the nuclear domain.

There are other standardization efforts related to individual technologies that are used in InX. For example, the 3GPP has set requirements for 5G systems used in industrial environments, such as service-level specifications (SLCs) for 5G technology-enabled connected industries, and enablers for industrial automation. Similarly, the 3GPP has also set technical specification groups (TSGs) to develop new standards for relevant technologies such as URLLC, and non-public networks. The TSG-SA working group (WG) 2 is responsible for specifications related to industries. The 5G Alliance for Connected Industries and Automation (ACIA) is meant to ensure the best possible applicability of 5G technology and networks for connected industries. Similarly, the 3GPP has also standardization activities related to CPS, IIoT, and machine learning, mainly to protect industrial data and systems from manipulation and security threats during communication. The specific output of the standardization organizations with a short description is presented in Table 4. Below, we discuss security features of the most important communication standards developed for industrial systems.

VIII. LESSONS LEARNED

This study sheds light on the revolutionary possibilities of new technologies in the development of InX. These technologies serve as the innovation accelerators for InX. The overall InX ecosystem is divided into three main parts, i.e., i) secure communications, ii) secure factory environment, and iii) industrial applications. The enabling technological components of each part are first introduced, followed by a detailed analysis of the security landscape of each technology. It is important to mention that the technological landscape in InX is huge, which cannot be covered in a single article. Therefore, the focus has been laid on selected crucial technologies that heavily rely on communications networks and technologies. Overall, the study emphasizes how crucial it is to investigate certain use cases to enforce security features related to these technologies in InX. Each of these enabling technologies brings with it specific security issues that need customized solutions. Examples of crucial factors to take into account are safeguarding IIoT and CPS devices against cyberattacks, organizing the enormous volumes of data in big data applications leveraging clouds, and maintaining the integrity of information through blockchain transactions. These lessons highlight the importance of having a thorough security plan that takes into account the unique characteristics of each developing technology and uses it to propel advancement toward InX. Below, we provide a summary of lessons learned in secure communications, secure factory environments, and industrial applications.

A. SECURITY OF COMMUNICATIONS

Since communications technologies make the backbone of InX, the security of communications technologies, such as 5G, and technologies used for communications-related computations including cloud and edge computing are highly important. For example, 5G wireless networks can expose industrial systems through the air interface to external threats. Similarly, important industrial information stored in cloud servers can expose sensitive critical information to third-party vendors, result in information leakage, or create bottlenecks and deadlocks during run-time due to congestion or DoS attacks.

UAV-based communications are considered extremely important in the realm of InX. However, due to limited computation capabilities, UAV-based communications will bring unique security challenges. Since industrial communications technologies were focused mainly during the fourth industrial revolution, various standard technologies will evolve for their use in InX. However, the security of those standards, such as MQTT, AMQP, and CoAP, to name a few, must also be improved to meet the needs of InX, where these technologies will be integrated with novel communications technologies, such as 5G, 5G advanced, and eventually 6G. Moreover, this study is limited to selected communications technologies, whereas the range of communication techniques can be huge in InX. In principle, however, security challenges must be first addressed independently within each technology and then within the integrated InX ecosystem.

B. SECURITY OF FACTORY ENVIRONMENT

The security of the factory environment is the most crucial and complicated one due to the amalgamation of a huge number of devices and technologies. Most technologies relying on IIoT and CPS, for instance, will also be vulnerable to security threats due to the inherent weaknesses of these technologies. For example, fingerprinting the firmware weaknesses in IIoT and CPS systems is an extremely daunting task on the one hand, and deploying strong security techniques is infeasible due to resource (e.g., computation) limitations, on the other hand. Similarly, collaborative robots will require extremely fast communication links, and a delay due to a security lapse, such as a man-in-the-middle attack, can cause huge damage. Therefore, specific research efforts are needed to strengthen the security of these technologies in InX.

The study provides important insights into the best practices for overseeing and controlling the enormous amounts of data in InX that are foundational for big data analytics and machine learning. A well-defined classification is essential to efficient data management since it keeps confidential data safe and well-organized. Further, a key component of data protection is the standardization of security mechanisms like encryption and access controls. A crucial factor to take into account is alignment with changing data privacy laws and compliance standards, which calls for constant watchfulness to make sure that data activities continue to comply with the law. The study highlights the importance of keeping abreast of emerging privacy regulations and cultivating an organizational culture of data responsibility. This will help InX navigate the complex data governance landscape while maintaining security and compliance standards. However, the study is limited to few enabling technologies which rely heavily on communications networks and technologies.

C. SECURITY OF INDUSTRIAL APPLICATIONS

The study provides important insights into the security of industrial applications. For example, blockchain technology can improve data-sharing security in InX. The decentralized and tamper-proof nature of blockchain technology promises to improve security by guaranteeing data integrity and lowering the possibility of unwanted changes. Auditability, being a crucial component of regulatory compliance inside InX, could be improved by the transparency and traceability of blockchain technology. However, the review also identifies important challenges. Processing requirements blockchains demand reliable infrastructure and energy-related concerns. To further optimize interoperability, security, governance, and consensus processes need to be in line with particular InX specifications. These lessons highlight the need for a well-bound strategy that highlights the security benefits of blockchain technology as well as the complex issues associated with its successful integration into InX's decentralized data-sharing system. Since the list of industrial applications can be extremely large, we have focused on two application scenarios as examples.

D. OVERALL SECURITY POSTURE OF INX

The thorough analysis in this review highlights the complex environment of InX, where the intersection of different technologies is crucial. As a result of the integration of cutting-edge technologies, InX depends on strong security policies, procedures, and techniques to safeguard and manage vital infrastructure and operations. The dynamic nature of threats demands that different security vulnerabilities must be addressed from the overall InX ecosystem perspective. InX can effectively manage the intricate cybersecurity problems it faces by promoting collaboration between different enabling technologies, guaranteeing the resilience of key infrastructures, and improving incident response capabilities. This synthesis highlights how crucial it is to take preventative measures to safeguard the transformational potential of InX and support its ongoing development in a society that is becoming more digitally linked and interconnected.

The study reveals that various security challenges are common to most enabling technologies of InX, irrespective of whether the technology belongs to communications, factory environments, or applications. For example, DoS attacks can happen on most centralized control entities in 5G, IIoT, and application servers in centralized clouds. Furthermore, a huge number of different kinds of IoT, CPS, and UAVs have been proposed and used for monitoring the conditions of systems in InX. Those systems rely on the communication infrastructure and monitoring tools that use the sensed data/information for further actions. Therefore, besides the inherent security challenges of each technology, such as IoT and CPS, the security challenges related to the communication infrastructure, data analytics, and machine learning, for instance, will have strong implications on the security of each technology using them. Therefore, it is important to investigate the security of each technology individually, as well as the whole end-to-end InX ecosystem in unison to ensure a secure ecosystem. Furthermore, non-conventional security approaches, appearing in the form of edge and fog computing to limit the computation of sensitive processes to local environments, must also be considered for improving the security of the whole InX ecosystem. Limiting the information flow to local industrial environments will surely increase the privacy of information compared to information flow over the Internet. Moreover, different attack models from different technologies can be used together to compromise the security of the integrated system. Overcoming such challenges will require strong defense techniques also working in unison to counter the combined attack force. Such a secure combination of different technologies will require further research from different aspects, as described in the following section.

IX. FUTURE RESEARCH DIRECTIONS

InX will be a shared and connected ecosystem driven by communication networks and technologies, mainly 5G and beyond (6G) wireless communication networks. In such a shared ecosystem, several relevant enabling technologies are required to have intelligent collaboration among each other to fulfill the dynamic needs of the InX applications. On the one hand, such integration of various key technologies may provide the needed flexibility and opportunities to build the desired network architecture and infrastructure for the applications of InX. On the other hand, the overall network will be highly complex which can lead to several challenges. One of the major challenges for such future networks will be to ensure the required degree of security and privacy and enable intelligent security services and trust among various involved entities/actors. Hence, this section is dedicated to putting some light on the potential future research directions in terms of securing various enabling technologies for communication in InX.

A. PERVASIVE AI

The evolution of telecom infrastructures towards 6G will include highly distributed AI, moving the intelligence from the central cloud closer to end nodes in the form of edge computing [386]. Distributed AI, aided by distributed edge and fog nodes and omnipresent radio technologies connecting those nodes, will complement the industrial process ahead of what has been envisioned by InX in many aspects. In addition to existing MEC-based solutions, where edge computing is managed at highly-capable server nodes integrated into the access network architecture, edge computing is envisioned to be extended towards local edge computing, where local nodes provide the needed computational capacity with collaborative effort [110]. The resulting three-tier computational architecture improves, e.g., resource efficiency by enabling the reduction of sensor data through local data analysis, reliability by ensuring the operation of critical services during network problems, and privacy by making it possible to process private and business-confidential data locally. The complexity of the resulting architecture, however, requires an increasing level of distributed intelligence at all levels to guarantee efficient, safe, secure, robust, and resilient services [386]. The majority of mission-critical and privacy-concerned applications of InX demand online distributed learning and training algorithms that can be employed at the edge devices [386]. Federated learning (FL) [387] is a promising paradigm for privacy-preserving distributed data training, enabling original datasets to be kept local while only the edge AI model parameters are shared [386]. Furthermore, DRL has shown good performance in various complicated EC scenarios [388]. Combining these two is an interesting research direction for InX. The combination of FL and DRL has already been studied by Shan et al. [389], where the FL framework was integrated with the mobile edge system to train DRL agents in a distributed way. From the viewpoint of security in InX, studying novel secure routing schemes and trust network topologies for edge intelligence service delivery while considering the coexistence of trusted edge nodes with malicious ones [386], would be an interesting research direction as well.

B. DATA SPACES

The concept of data space has gained prominence with European initiatives to develop a reference architecture for secure data exchange and data sovereignty. In the frame of InX, we can expect greater decentralization and higher complexity. Thus, for future operations, management and intelligent decision-making more interfaces need to be integrated. This integration should happen based on data space concepts as represented by the Industrial Data Space and Gaia-X [390]. With a corresponding reference architecture for secure data exchange and trustworthy data sharing, IDS and Gaia-X contribute to the digitization of industry and its further evolution. One goal is to accommodate the decentralization of industrial architectures, as is the case in supply chains, for example, and to bridge the limitations of top-down approaches, both in technological terms and concerning the needs of industry, politics, and standardization [391]. Through the architecture, different cloud platforms can be connected without losing or compromising secure data exchange or control over the data. The mechanisms of the architecture place the principle of data sovereignty at the center. Arguably the most important component is the connector, which links enterprise architectures or even individual, networked devices to data space, and ensures the identity and integrity of the connected software systems and components [392]. The result is a federated system characterized by trustworthiness, transparency, and interoperability, relying on existing and evolving standards [393]. Decentralized data sharing promises to enhance data fluidity by facilitating smooth data sharing and cooperation between various InX components. System reliability is improved by the inherent resilience of decentralized networks, which reduces the possibility of single points of failure. The evolution towards InX will depend on the ability of the industry to exploit data and become part of the data economy. Therefore, it will be crucial to understand the impact of the data space concept on industrial operations and future business models and to create the data spaces needed for industrial development [394].

C. AUGMENTED REALITY

So far, the focus has been to deliver technologies that make IAR applications a possibility to support various industrial processes. These applications require different mobile devices including smartphones, tablets, PCs, Google glasses, or Microsoft HoleLens. These devices require different types of security systems and procedures. Among the most pressing challenges that need further research is the security and privacy of transmitted video and audio between a remote location and InX facilities. Furthermore, multi-modal authentication on IAR devices [332] is needed. Protecting collaborative interactions among parties providing live remote support and local operators needs further investigation. Since the domain of IAR is still not widely adopted, there is a high possibility that new security challenges will arise with the wide adoption of the technology. Hence, more research on proactively investigating the potential exposure from IAR is needed. The principle of security-by-design must be adopted in designing new IAR applications, services, and devices due to the extremely serious nature of the involved resources.

D. ADVANCED ROBOTICS

As robot systems rise in importance for both industry and consumers, also the risk of security threats exploiting vulnerabilities from either hardware or software. Security by design is an approach that requires the consideration of security requirements for robotics applications starting in early development phases and the whole life cycle [395], thus increasing trustworthiness. In [396], the authors state how the monitoring and tracking of privileged accounts can help to estimate and mitigate the impact of a security breach. Anomaly detection and robot behavior fingerprinting are promising research directions that will help with controlling data usage and robotic systems identification. Finally, improving authentication, authorization, and encryption in robotics frameworks is a must, and ROS has the upper hand in this aspect. With the advent of ROS2 (a merging of DDS and ROS), research toward the next security phases is possible.

E. VISIBLE LIGHT COMMUNICATIONS

Extremely high data rates with extremely low latency can be provided by Visible Light Communications (VLC) technologies [397]. Factory floors lit by VLC, providing super-fast connectivity, will extend sustainable communications to actuators and robotic arms, mainly because the existing challenges of VLC such as distance and shadow effects will not exist on factory floors. Therefore, VLC makes one of the best high-data rate dual-function data delivery technology. However, more research is needed on the integration aspects of VLC into equipment that may not look suitable for VLC, for instance, due to its fragile nature. The security aspects of VLC in InX are more from the physical layer perspective, as discussed in [398], due to the nature of the technology needing line-of-sight, and use cases of InX related to indoor environments and components.

F. DATA SOVEREIGNTY

Data sovereignty [399], i.e., self-authority on the control of data including its use and dissemination, is very important. Data sovereignty enables managing information in a way that is consistent with the laws, practices, and customs of the state where the data is located [399]. There are various approaches to ensuring data sovereignty including technical and legislative methods. Among the latter, various organizations have been formed such as the International Data Spaces (IDSs) [400], which has also developed a reference architecture that ensures data sovereignty besides the security and privacy of data. The IDS also enables the sharing of data in a contract-binding and safe methodology among the corporate sectors while storing the data in virtual spaces [401].

G. AUTOMATION OF EVERYTHING FOR SECURITY

Industrial automation from the connectivity perspective is a high research topic, as discussed in [244]. The automation of networked systems in InX will be inevitable. Machine execution of complex functions or in other words, automation is used for i) information acquisition, ii) information analysis, iii) decision and action selection, and iv) action implementation for accuracy and reliability [402]. The complexity in communication networks due to heterogeneity in networks, devices, applications, and services along with its criticality in InX forces us to automate network operations [403], [404]. Network management becomes complicated as the network grows, and security policy enforcement with adjusting increasing numbers of parameters further complicates the whole management. Since, human-machine interaction has been a major reason for the network downtime [405] with security lapses as a consequence [209], [406], due to manual configuration of network security technologies [407], [408], automation of security of InX becomes an eminent research area. One interesting aspect related to automation that needs multi-disciplinary research is the right balance between human and machine control, as discussed in [79].

H. SOFTWARE-DEFINED MACHINES

Software-defined machines (SDMs) bring new opportunities to InX, may that be manufacturing, assembly lines, or simply factory floor mobility. The basic concept behind SDM is that machines can be configured at run-time for different functionalities by externalizing the control and processing functions [409]. Such externalizing would require efficient communications technologies with robust security in place. Since 6G aims to provide ubiquitous connectivity, securing SDMs will be extremely important. To understand the importance of the security of SDMs, consider the case of successful rogue attempts that can enable, for instance, robotic arms to cause damage on the factory floor. Therefore, the security of SDMs in InX in the era of 6G makes an interesting research area.

X. CONCLUSION

In this article, we highlighted the security landscape of communications in InX. The main security challenges that can arise from using the most enabling technologies of InX are elaborated followed by potential solutions. Since InX will use novel technologies that will share, send or receive information over communication networks, the security challenges that exist in communications networks will have serious consequences on the security of those technologies, and as a result on InX. For example, CPS, IoT, and machine learning, to name a few, will need to send or receive data. Hence, the security of the communication media or network and computational architecture will have direct implications on the working of CPS, IoT, and machine learning algorithms. Since this area has not been previously explored from the communications security perspective, it is highly important to shed light on security concerns, possible solutions, and existing gaps to stir further research in this direction. This article also provides important insights into future research directions in the domain of InX, to motivate research beyond the current state-of-the-art into the 6G era for InX.

REFERENCES

[1] M. A. Yülek, *The Industrialization Process: A Streamlined Version*. Singapore: Springer, 2018, pp. 171–182. [Online]. Available: https://doi.org/10.1007/978-981-13-0568-9_8

[2] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann, “Industry 4.0,” *Bus. Inf. Syst. Eng.*, vol. 6, no. 4, pp. 239–242, 2014.

[3] K. Zhou, T. Liu, and L. Zhou, "Industry 4.0: Towards future industrial opportunities and challenges," in *Proc. 12th Int. Conf. Fuzzy Syst. Knowl. Disc. (FSKD)*, 2015, pp. 2147–2152.

[4] K. A. Demir, G. Döven, and B. Sezen, "Industry 5.0 and human–robot co-working," *Procedia Comput. Sci.*, vol. 158, pp. 688–695, Oct. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050919312748

[5] "Industry 5.0. European Commission." 2023. [Online]. Available: https://ec.europa.eu/info/research-and-innovation/research-area/industrial-research-and-innovation/industry-50_en

[6] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The future of industrial communication: Automation networks in the era of the Internet of Things and industry 4.0," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 17–27, Mar. 2017.

[7] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Commun. Stand. Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 2018.

[8] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *Comprehensive Guide to 5G Security*. Hoboken, NJ, USA: Wiley, 2018.

[9] H. Farag, E. Sisinni, M. Gidlund, and P. Österberg, "Priority-aware wireless fieldbus protocol for mixed-criticality industrial wireless sensor networks," *IEEE Sensors J.*, vol. 19, no. 7, pp. 2767–2780, Apr. 2019.

[10] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2017, pp. 193–199.

[11] J. Jasperneite, T. Sauter, and M. Wollschlaeger, "Why we need automation models: Handling complexity in industry 4.0 and the Internet of Things," *IEEE Ind. Electron. Mag.*, vol. 14, no. 1, pp. 29–40, Mar. 2020.

[12] R. Drath and A. Horch, "Industrie 4.0: Hit or hype? [Industry forum]," *IEEE Ind. Electron. Mag.*, vol. 8, no. 2, pp. 56–58, Jun. 2014.

[13] F. Chiarello, L. Trivelli, A. Bonaccorsi, and G. Fantoni, "Extracting and mapping industry 4.0 technologies using wikipedia," *Comput. Ind.*, vol. 100, pp. 244–257, Sep. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0166361517306176

[14] G. Reischauer, "Industry 4.0 as policy-driven discourse to institutionalize innovation systems in manufacturing," *Technol. Forecast. Social Change*, vol. 132, pp. 26–33, Jul. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0040162517316657

[15] S. Wang, J. Wan, D. Li, and C. Zhang, "Implementing smart factory of industrie 4.0: An outlook," *Int. J. Distrib. Sens. Netw.*, vol. 12, no. 1, 2016, Art. no. 3159805.

[16] M. Hermann, T. Pentek, and B. Otto, "Design principles for Industrie 4.0 scenarios," in *Proc. 49th Hawaii Int. Conf. Syst. Sci. (HICSS)*, 2016, pp. 3928–3937.

[17] S. Hollerer, T. Sauter, and W. Kastner, "Risk assessments considering safety, security, and their interdependencies in OT environments," in *Proc. 17th Int. Conf. Availability, Rel. Security*, New York, NY, USA, 2022, p. 94. [Online]. Available: https://doi.org/10.1145/3538969.3543814

[18] *Industry 5.0: Towards More Sustainable, Resilient and Human-Centric Industry: Directorate-General for Research and Innovation*, Eur. Comm., Brussels, Belgium, 2021.

[19] B. Walker, C. S. Holling, S. R. Carpenter, and A. Kinzig, "Resilience, adaptability and transformability in social–ecological systems," *Ecol. Soc.*, vol. 9, no. 2, p. 5, 2004.

[20] P.-C. Lee, S.-H. Chen, Y.-S. Lin, and H.-N. Su, "Toward a better understanding on technological resilience for sustaining industrial development," *IEEE Trans. Eng. Manag.*, vol. 66, no. 3, pp. 398–411, Aug. 2019.

[21] D. Paschek, C.-T. Luminosu, and E. Ocakci, "Industry 5.0 challenges and perspectives for manufacturing systems in the society 5.0," in *Sustainability and Innovation in Manufacturing Enterprises*. Singapore: Springer, 2022, pp. 17–63.

[22] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, 4th Quart., 2019.

[23] D. Jeong, "Artificial intelligence security threat, crime, and forensics: Taxonomy and open issues," *IEEE Access*, vol. 8, pp. 184560–184574, 2020.

[24] Q. Wang and J. Jiang, "Comparative examination on architecture and protocol of industrial wireless sensor network standards," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2197–2219, 3rd Quart., 2016.

[25] O. B. Sezer, E. Dogdu, and A. M. Ozbayoglu, "Context-aware computing, learning, and big data in Internet of Things: A survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 1–27, Feb. 2018.

[26] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—A survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017.

[27] A. Burg, A. Chattopadhyay, and K.-Y. Lam, "Wireless communication and security issues for cyber–physical systems and the Internet-of-Things," *Proc. IEEE*, vol. 106, no. 1, pp. 38–60, Jan. 2018.

[28] J. Li, F. R. Yu, G. Deng, C. Luo, Z. Ming, and Q. Yan, "Industrial Internet: A survey on the enabling technologies, applications, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1504–1526, 3rd Quart., 2017.

[29] M. Langfinger, M. Schneider, D. Stricker, and H. D. Schotten, "Addressing security challenges in industrial augmented reality systems," in *Proc. IEEE 15th Int. Conf. Ind. Inform. (INDIN)*, 2017, pp. 299–304.

[30] S. R. Chhetri, N. Rashid, S. Faezi, and M. A. A. Faruque, "Security trends and advances in manufacturing systems in the era of industry 4.0," in *Proc. 36th Int. Conf. Comput.-Aided Design*, 2017, pp. 1039–1046.

[31] Q. Liu, P. Li, W. Zhao, W. Cai, S. Yu, and V. C. M. Leung, "A survey on security threats and defensive techniques of machine learning: A data driven view," *IEEE Access*, vol. 6, pp. 12103–12117, 2018.

[32] M. Mamdouh, M. A. I. Elrukhsi, and A. Khattab, "Securing the Internet of Things and wireless sensor networks via machine learning: A survey," in *Proc. Int. Conf. Comput. Appl. (ICCA)*, Aug. 2018, pp. 215–218.

[33] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018.

[34] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3453–3495, 4th Quart., 2018.

[35] A. Martín, E. Soriano, and J. Cañas, "Quantitative analysis of security in distributed robotic frameworks," *Robot. Auton. Syst.*, vol. 100, pp. 95–107, Feb. 2018.

[36] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, Jan. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925231217316351

[37] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019.

[38] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1636–1675, 2nd Quart., 2019.

[39] T. P. Raptis, A. Passarella, and M. Conti, "Data management in industry 4.0: State of the art and open challenges," *IEEE Access*, vol. 7, pp. 97052–97093, 2019.

[40] G. Aceto, V. Persico, and A. Pescape, "A survey on information and communication technologies for industry 4.0: State-of-the-art, taxonomies, perspectives, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3467–3501, 4th Quart., 2019.

[41] S. Jarin and R. Doriya, "Security issues and solutions in cloud robotics: A survey," in *Next Generation Computing Technologies on Computational Intelligence*. Singapore: Springer, 2019.

[42] X. Sun, D. Ng, Z. Ding, Y. Xu, and Z. Zhong, "Physical layer security in UAV systems: Challenges and opportunities," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 40–47, Oct. 2019.

[43] M. M. Alani and M. Alloghani, *Security Challenges in the Industry 4.0 Era*. Cham, Switzerland: Springer Int., 2019, pp. 117–136. [Online]. Available: https://doi.org/10.1007/978-3-030-12953-8_8

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

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

[46] O. A. Alimi, K. Ouahada, and A. M. Abu-Mahfouz, "A review of machine learning approaches to power system security and stability," *IEEE Access*, vol. 8, pp. 113512–113531, 2020.

[47] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on SCADA systems: Secure protocols, incidents, threats and tactics," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1942–1976, 3rd Quart., 2020.

[48] T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, and D. O. Wu, "Edge computing in Industrial Internet of Things: Architecture, advances and challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2462–2488, 4th Quart., 2020.

[49] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, "A survey of honeypots and honeynets for Internet of Things, Industrial Internet of Things, and cyber-physical systems," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2351–2383, 4th Quart., 2021.

[50] D. Zhang, Q.-G. Wang, G. Feng, Y. Shi, and A. V. Vasilakos, "A survey on attack detection, estimation and control of industrial cyber–physical systems," *ISA Trans.*, vol. 116, pp. 1–16, Oct. 2021.

[51] H. Kayan, M. Nunes, O. Rana, P. Burnap, and C. Perera, "Cybersecurity of industrial cyber-physical systems: A review," *ACM Comput. Surveys*, vol. 54, no. 11S, pp. 1–35, 2022.

[52] A. Verma et al., "Blockchain for industry 5.0: Vision, opportunities, key enablers, and future directions," *IEEE Access*, vol. 10, pp. 69160–69199, 2022.

[53] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, "Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review," *Comput. Ind.*, vol. 137, May 2022, Art. no. 103614.

[54] R. Muzaffar, M. Ahmed, E. Sisinni, T. Sauter, and H.-P. Bernhard, "5G deployment models and configuration choices for industrial cyber-physical systems—A state of art overview," *IEEE Trans. Ind. Cyber-Phys. Syst.*, vol. 1, pp. 236–256, 2023.

[55] X. Etxezarreta, I. Garitano, M. Iturbe, and U. Zurutuza, "Software-defined networking approaches for intrusion response in industrial control systems: A survey," *Int. J. Crit. Infrastruct. Protect.*, vol. 42, Sep. 2023, Art. no. 100615.

[56] S. M. Khalil, H. Bahsi, and T. Korõtko, "Threat modeling of industrial control systems: A systematic literature review," *Comput. Security*, vol. 136, Jan. 2024, Art. no. 103543.

[57] T. Sauter and A. Treytl, "IoT-enabled sensors in automation systems and their security challenges," *IEEE Sens. Lett.*, vol. 7, no. 12, pp. 1–4, Dec. 2023.

[58] Y. Wu, H. N. Dai, and H. Wang, "Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2300–2317, Feb. 2021.

[59] M. Conti, D. Donadel, and F. Turrin, "A survey on industrial control system testbeds and datasets for security research," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2248–2294, 4th Quart., 2021.

[60] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," *Comput. Security*, vol. 89, Feb. 2020, Art. no. 101677.

[61] D. Bailey and E. Wright, *Practical SCADA for Industry*. Amsterdam, The Netherlands: Elsevier, 2003.

[62] A. Homay, C. Chrysoulas, B. El Boudani, M. de Sousa, and M. Wollschlaeger, "A security and authentication layer for SCADA/DCS applications," *Microprocess. Microsyst.*, vol. 87, Nov. 2021, Art. no. 103479.

[63] S. Ghosh and S. Sampalli, "A survey of security in SCADA networks: Current issues and future challenges," *IEEE Access*, vol. 7, pp. 135812–135831, 2019.

[64] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network function virtualization: Challenges and opportunities for innovations," *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 90–97, Feb. 2015.

[65] F. Hu, Q. Hao, and K. Bao, "A survey on software defined networking (SDN) and OpenFlow: From concept to implementation," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 2181–2206, 4th Quart., 2014.

[66] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "security in software defined networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2317–2346, 4th Quart., 2015.

[67] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[68] C. Greer, M. Burns, D. Wollman, and E. Griffor, "Cyber-physical systems and Internet of Things," NIST, Gaithersburg, MA, USA, Rep. NIST SP 1900-201, 2019.

[69] Q. Qi and F. Tao, "Digital twin and big data towards smart manufacturing and industry 4.0: 360 degree comparison," *IEEE Access*, vol. 6, pp. 3585–3593, 2018.

[70] O. Müller, M. Fay, and J. vom Brocke, "The effect of big data and analytics on firm performance: An econometric analysis considering industry characteristics," *J. Manage. Inf. Syst.*, vol. 35, no. 2, pp. 488–509, 2018.

[71] J. H. Kim, "A review of cyber-physical system research relevant to the emerging IT trends: Industry 4.0, IoT, big data, and cloud computing," *J. Ind. Integr. Manage.*, vol. 2, no. 3, 2017, Art. no. 1750011.

[72] M. Hammer, K. Somers, H. Karre, and C. Ramsauer, "Profit per hour as a target process control parameter for manufacturing systems enabled by big data analytics and industry 4.0 infrastructure," *Procedia CIRP*, vol. 63, pp. 715–720, Jul. 2017.

[73] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804510001281

[74] G. Ramachandra, M. Iftikhar, and F. A. Khan, "A comprehensive survey on security in cloud computing," *Procedia Comput. Sci.*, vol. 110, pp. 465–472, Jul. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050917313030

[75] K. Gai, J. Guo, L. Zhu, and S. Yu, "Blockchain meets cloud computing: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 2009–2030, 3rd Quart., 2020.

[76] V. Del Piccolo, A. Amamou, K. Haddadou, and G. Pujolle, "A survey of network isolation solutions for multi-tenant data centers," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2787–2821, 4th Quart., 2016.

[77] J. Men, Z. Lv, X. Zhou, Z. Han, H. Xian, and Y. Song, "Machine learning methods for industrial protocol security analysis: Issues, taxonomy, and directions," *IEEE Access*, vol. 8, pp. 83842–83857, 2020.

[78] J. Suomalainen, A. Juhola, S. Shahabuddin, A. Mämmelä, and I. Ahmad, "Machine learning threatens 5G security," *IEEE Access*, vol. 8, pp. 190822–190842, 2020.

[79] M. G. Kibria, K. Nguyen, G. P. Villardi, O. Zhao, K. Ishizu, and F. Kojima, "Big data analytics, machine learning and artificial intelligence in next-generation wireless networks," *IEEE Access*, vol. 6, pp. 32328–32338, 2018.

[80] A. Fotouhi, H. Qiang, L. Giordano, A. Garcia-Rodriguez, and J. Yuan, "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3417–3442, 4th Quart., 2019.

[81] J. Yaacoub, H. Naura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet Things*, vol. 11, Sep. 2020, Art. no. 100218.

[82] N. Khan, S. Brohi, and N. Jhanijhi, *Intelligent Computing and Innovation on Data Science*. Singapore: Springer, 2020.

[83] N. DeMarinis, S. Tellex, V. Kemerlis, G. Konidaris, and R. Fonseca, "Scanning the Internet for ROS: A view of security in robotics research," in *Proc. Int. Conf. Robot. Autom. (ICRA)*, vol. 11, 2019, pp. 8514–8521.

[84] C. Archivald, L. Schwalm, and J. Ball, "A survey of security in robotic systems: Vulnerabilities, attacks, and solutions," *Int. J. Robot. Autom.*, vol. 32, pp. 1–7, Jan. 2017.

[85] P. Fraga-Lamas, T. M. FernáNdez-Caramés, Ó. Blanco-Novoa, and M. A. Vilar-Montesinos, "A review on industrial augmented reality systems for the industry 4.0 shipyard," *IEEE Access*, vol. 6, pp. 13358–13375, 2018.

[86] P. Fraga-Lamas, J. Varela-Barbeito, and T. M. Fernández-Caramés, "Next generation auto-identification and traceability technologies for industry 5.0: A methodology and practical use case for the shipbuilding industry," *IEEE Access*, vol. 9, pp. 140700–140730, 2021.

[87] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 858–880, 1st Quart., 2018.

[88] J. Leng, M. Zhou, L. J. Zhao, Y. Huang, and Y. Bian, "Blockchain security: A survey of techniques and research directions," *IEEE Trans. Services Comput.*, vol. 15, no. 4, pp. 2490–2510, Jul./Aug. 2022.

[89] J. Leng et al., "Blockchain-secured smart manufacturing in industry 4.0: A survey," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 1, pp. 237–252, Jan. 2021.

[90] P. Zhuang, T. Zamir, and H. Liang, "Blockchain for cybersecurity in smart grid: A comprehensive survey," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 3–19, Jan. 2021.

[91] R. Gupta, S. Tanwar, N. Kumar, and S. Tyagi, "Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review," *Comput. Elect. Eng.*, vol. 86, Sep. 2020, Art. no. 106717.

[92] I. Homoliak, S. Venugopalan, D. Reijsbergen, Q. Hum, R. Schumi, and P. Szalachowski, "The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 341–390, 1st Quart., 2021.

[93] B. Bhushan, P. Sinha, K. M. Sagayam, and J. Andrew, "Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions," *Comput. Electr. Eng.*, vol. 90, Mar. 2021, Art. no. 106897.

[94] M. Saad et al., "Exploring the attack surface of blockchain: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1977–2008, 3rd Quart., 2020.

[95] H. Hasanova, U.-J. Baek, M.-G. Shin, K. Cho, and M.-S. Kim, "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures," *Int. J. Netw. Manage.*, vol. 29, no. 2, 2019, Art. no. e2060.

[96] D. Dasgupta, J. M. Shrein, and K. D. Gupta, "A survey of blockchain from security perspective," *J. Banking Financ. Technol.*, vol. 3, no. 1, pp. 1–17, 2019.

[97] U. Bodkhe et al., "Blockchain for industry 4.0: A comprehensive review," *IEEE Access*, vol. 8, pp. 79764–79800, 2020.

[98] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on Industrial Internet of Things: A cyber-physical systems perspective," *IEEE Access*, vol. 6, pp. 78238–78259, 2018.

[99] A. Aadhityan, "A novel method for implementing artificial intelligence, cloud and Internet of Things in robots," in *Proc. Int. Conf. Innov. Inf., Embedded Commun. Syst. (ICIIECS)*, 2015, pp. 1–4.

[100] S. Earley, "Analytics, machine learning, and the Internet of Things," *IT Prof.*, vol. 17, no. 1, pp. 10–13, Jan./Feb. 2015.

[101] M. Marjani et al., "Big IoT data analytics: Architecture, opportunities, and open research challenges," *IEEE Access*, vol. 5, pp. 5247–5261, 2017.

[102] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[103] A. R. Biswas and R. Giaffreda, "IoT and cloud convergence: Opportunities and challenges," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 375–376.

[104] A. Varghese and D. Tandur, "Wireless requirements and challenges in industry 4.0," in *Proc. Int. Conf. Contemporary Comput. Inform. (IC3I)*, 2014, pp. 634–638.

[105] R. Sanchez-Iborra and M.-D. Cano, "State of the art in LP-WAN solutions for industrial IoT services," *Sensors*, vol. 16, no. 5, p. 708, 2016.

[106] A. Mahmood, S. F. Abedin, T. Sauter, M. Gidlund, and K. Landernäs, "Factory 5G: A review of industry-centric features and deployment options," *IEEE Ind. Electron. Mag.*, vol. 16, no. 2, pp. 24–34, Jun. 2022.

[107] G. Brown et al., *Ultra-reliable Low-Latency 5G for Industrial Automation*, vol. 2, Qualcomm, San Diego, CA, USA, 2018, Art. no. 52065394.

[108] S. A. Ashraf, I. Aktas, E. Eriksson, K. W. Helmersson, and J. Ansari, "Ultra-reliable and low-latency communication for wireless factory automation: From LTE to 5G," in *Proc. IEEE 21st Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, 2016, pp. 1–8.

[109] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computing—A key technology towards 5G," vol. 11, ETSI, Sophia Antipolis, France, White Paper, 2015.

[110] E. Harjula et al., "Decentralized IoT edge nanoservice architecture for future gadget-free computing," *IEEE Access*, vol. 7, pp. 119856–119872, 2019.

[111] G. Lee, W. Saad, and M. Bennis, "Online optimization for UAV-assisted distributed fog computing in smart factories of industry 4.0," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2018, pp. 1–6.

[112] L. Thames and D. Schaefer, *Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing*. Cham, Switzerland: Springer, 2017.

[113] L. Atzori, A. Iera, and G. Morabito, "From 'smart objects' to 'social objects': The next evolutionary step of the Internet of Things," *IEEE Commun. Mag.*, vol. 52, no. 1, pp. 97–105, Jan. 2014.

[114] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X13000241

[115] D. Sempreboni and L. Viganò, "Privacy, security and trust in the Internet of neurons," 2018, *arXiv:1807.06077*.

[116] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The Industrial Internet of Things (IIoT): An analysis framework," *Comput. Ind.*, vol. 101, pp. 1–12, Oct. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0166361517307285

[117] J. Okwuibe, J. Haavisto, E. Harjula, I. Ahmad, and M. Ylianttila, "SDN enhanced resource orchestration of containerized edge applications for industrial IoT," *IEEE Access*, vol. 8, pp. 229117–229131, 2020.

[118] I. Ahmad et al., "Towards gadget-free Internet services: A roadmap of the naked world," *Telematics Inform.*, vol. 35, no. 1, pp. 82–92, 2018.

[119] T. Kumar, P. Porambage, I. Ahmad, M. Liyanage, E. Harjula, and M. Ylianttila, "Securing gadget-free digital services," *Computer*, vol. 51, no. 11, pp. 66–77, Nov. 2018.

[120] A. Grau, M. Indri, L. Lo Bello, and T. Sauter, "Robots in industry: The past, present, and future of a growing collaboration with humans," *IEEE Ind. Electron. Mag.*, vol. 15, no. 1, pp. 50–61, Mar. 2021.

[121] A. Rahman, J. Jin, A. Cricenti, A. Rahman, and D. Yuan, "A cloud robotics framework of optimal task offloading for smart city applications," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2016, pp. 1–7.

[122] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, "Fog computing: A platform for Internet of Things and analytics," in *Big Data and Internet of Things: A Roadmap for Smart Environments*. Cham, Switzerland: Springer, 2014, pp. 169–186.

[123] I. Ahmad et al., "Machine learning meets communication networks: Current trends and future challenges," *IEEE Access*, vol. 8, pp. 223418–223460, 2020.

[124] X. Xu, Y. Lu, B. Vogel-Heuser, and L. Wang, "Industry 4.0 and industry 5.0—Inception, conception and perception," *J. Manuf. Syst.*, vol. 61, pp. 530–535, Oct. 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0278612521002119

[125] P. Patel, M. I. Ali, and A. Sheth, "On using the intelligent edge for IoT analytics," *IEEE Intell. Syst.*, vol. 32, no. 5, pp. 64–69, Sep./Oct. 2017.

[126] J. Park, S. Samarakoon, M. Bennis, and M. Debbah, "Wireless network intelligence at the edge," *Proc. IEEE*, vol. 107, no. 11, pp. 2204–2239, Nov. 2019.

[127] A. Diez-Olivan, J. Del Ser, D. Galar, and B. Sierra, “Data fusion and machine learning for industrial prognosis: Trends and perspectives towards industry 4.0,” *Inf. Fusion*, vol. 50, pp. 92–111, Oct. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1566253518304706

[128] P. K. R. Maddikunta et al., “Industry 5.0: A survey on enabling technologies and potential applications,” *J. Ind. Inf. Integr.*, vol. 26, Mar. 2022, Art. no. 100257. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2452414X21000558

[129] T. Masood and J. Egger, “Augmented reality in support of industry 4.0—Implementation challenges and success factors,” *Robot. Comput.-Integr. Manuf.*, vol. 58, pp. 181–195, Aug. 2019.

[130] F. De Pace, F. Manuri, and A. Sanna, “Augmented reality in industry 4.0,” *Amer. J. Comput. Sci. Inf. Technol.*, vol. 6, no. 1, p. 17, 2018.

[131] J. Al-Jaroodi and N. Mohamed, “Blockchain in industries: A survey,” *IEEE Access*, vol. 7, pp. 36500–36515, 2019.

[132] R. Liu, X. Yu, Y. Yuan, and Y. Ren, “BTDSI: A blockchain-based trusted data storage mechanism for industry 5.0,” *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 8, 2023, Art. no. 101674.

[133] P. Centobelli, R. Cerchione, P. Del Vecchio, E. Oropallo, and G. Secundo, “Blockchain technology for bridging trust, traceability and transparency in circular supply chain,” *Inf. Manag.*, vol. 59, no. 7, 2022, Art. no. 103508.

[134] F. Spinelli and V. Mancuso, “Toward enabled industrial verticals in 5G: A survey on MEC-based approaches to provisioning and flexibility,” *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 596–630, 1st Quart., 2021.

[135] N. Dao, Y. Lee, S. Cho, E. Kim, K. Chung, and C. Keum, “Multitier multi-access edge computing: The role for the fourth industrial revolution,” in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, 2017, pp. 1280–1282.

[136] R. Muñoz et al., “Integration of IoT, transport SDN, and edge/cloud computing for dynamic distribution of IoT analytics and efficient use of network resources,” *J. Lightw. Technol.*, vol. 36, no. 7, pp. 1420–1428, Apr. 1, 2018.

[137] A. R. Curtis, J. C. Mogul, J. Tourrilhes, P. Yalagandula, P. Sharma, and S. Banerjee, “DevoFlow: Scaling flow management for high-performance networks,” in *Proc. ACM SIGCOMM Conf.*, 2011, pp. 254–265.

[138] R. Fujdiak et al., “On track of Sigfox confidentiality with end-to-end encryption,” in *Proc. 13th Int. Conf. Availability, Rel. Security*, 2018, pp. 1–6. [Online]. Available: https://doi.org/10.1145/3230833.3232805

[139] H. Xu, P. V. Klaine, O. Onireti, B. Cao, M. Imran, and L. Zhang, “Blockchain-enabled resource management and sharing for 6G communications,” *Digit. Commun. Netw.*, vol. 6, no. 3, pp. 261–269, 2020.

[140] P. Radanliev et al., “Integration of cyber security frameworks, models and approaches for building design principles for the Internet-of-Things in industry 4.0,” in *Proc. Living Internet Things Cybersecurity IoT*, 2018, pp. 1–6.

[141] R. A. A. Habeeb, F. Nasaruddin, A. Gani, I. A. T. Hashem, E. Ahmed, and M. Imran, “Real-time big data processing for anomaly detection: A survey,” *Int. J. Inf. Manage.*, vol. 45, pp. 289–307, Apr. 2019.

[142] A. Meshram and C. Haas, “Anomaly detection in industrial networks using machine learning: A roadmap,” in *Machine Learning for Cyber Physical Systems*. Heidelberg, Germany: Springer, 2017, pp. 65–72.

[143] S. D. D. Anton, S. Sinha, and H. D. Schotten, “Anomaly-based intrusion detection in industrial data with SVM and random forests,” in *Proc. Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM)*, 2019, pp. 1–6.

[144] Y. Wu et al., “A comparative measurement study of deep learning as a service framework,” *IEEE Trans. Services Comput.*, vol. 15, no. 1, pp. 551–566, Jan./Feb. 2022.

[145] F. Tramèr, A. Kurakin, N. Papernot, I. Goodfellow, D. Boneh, and P. McDaniel, “Ensemble adversarial training: Attacks and defenses,” 2017, *arXiv:1705.07204*.

[146] P. Zhao, H. Huang, X. Zhao, and D. Huang, “P3: Privacy-preserving scheme against poisoning attacks in mobile-edge computing,” *IEEE Trans. Comput. Social Syst.*, vol. 7, no. 3, pp. 818–826, Jun. 2020.

[147] K. Bonawitz et al., “Practical secure aggregation for privacy-preserving machine learning,” in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, New York, NY, USA, 2017, pp. 1175–1191. [Online]. Available: http://doi.acm.org/10.1145/3133956.3133982

[148] B. Wang et al., “Neural cleanse: Identifying and mitigating backdoor attacks in neural networks,” in *Proc. IEEE Symp. Security Privacy (SP)*, 2019, pp. 707–723.

[149] M. Abadi et al., “Deep learning with differential privacy,” in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 308–318. [Online]. Available: https://doi.org/10.1145/2976749.2978318

[150] Z. Liu, K. R. Choo, and J. Grossschadl, “Securing edge devices in the post-quantum Internet of Things using lattice-based cryptography,” *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 158–162, Feb. 2018.

[151] R. Hsu, J. Lee, T. Q. S. Quek, and J.-C. Chen, “Reconfigurable security: Edge-computing-based framework for IoT,” *IEEE Netw.*, vol. 32, no. 5, pp. 92–99, Sep./Oct. 2018.

[152] Y. Chen, Y. Zhang, S. Maharjan, M. Alam, and T. Wu, “Deep learning for secure mobile edge computing in cyber-physical transportation systems,” *IEEE Netw.*, vol. 33, no. 4, pp. 36–41, Jul./Aug. 2019.

[153] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, “Data security and privacy-preserving in edge computing paradigm: Survey and open issues,” *IEEE Access*, vol. 6, pp. 18209–18237, 2018.

[154] I. Sluganovic, M. Serbec, A. Derek, and I. Martinovic, “HoloPair: Securing shared augmented reality using microsoft HoloLens,” in *Proc. 33rd Annu. Comput. Security Appl. Conf.*, 2017, pp. 250–261.

[155] J. Shang and J. Wu, “Enabling secure voice input on augmented reality headsets using internal body voice,” in *Proc. 16th Annu. IEEE Int. Conf. Sens., Commun. Netw. (SECON)*, 2019, pp. 1–9.

[156] E. Gaebel, N. Zhang, W. Lou, and Y. T. Hou, “Looks good to me: Authentication for augmented reality,” in *Proc. 6th Int. Workshop Trustworthy Embedded Devices*, 2016, pp. 57–67.

[157] P. Otte, M. de Vos, and J. Pouwelse, “TrustChain: A Sybil-resistant scalable blockchain,” *Future Gener. Comput. Syst.*, vol. 107, pp. 770–780, Jun. 2020.

[158] P. Swathi, C. Modi, and D. Patel, “Preventing Sybil attack in blockchain using distributed behavior monitoring of miners,” in *Proc. 10th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, 2019, pp. 1–6.

[159] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, “An ID-based linearly homomorphic signature scheme and its application in blockchain,” *IEEE Access*, vol. 6, pp. 20632–20640, 2018.

[160] M. Signorini, M. Pontecorvi, W. Kanoun, and R. Di Pietro, “BAD: A blockchain anomaly detection solution,” *IEEE Access*, vol. 8, pp. 173481–173490, 2020.

[161] M. Signorini, M. Pontecorvi, W. Kanoun, and R. Di Pietro, “ADvISE: Anomaly detection tool for blockchaIn SystEms,” in *Proc. IEEE World Congr. Services (Services)*, 2018, pp. 65–66.

[162] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, “Eclipse attacks on bitcoin’s peer-to-peer network,” in *Proc. 24th USENIX Security Symp. (USENIX Security)*, 2015, pp. 129–144.

[163] S. Hopkins, C. Henry, S. Bagui, A. Mishra, E. Kalaimannan, and C. S. John, “Applying a verified trusted computing base to Cyber protect a vulnerable traffic control cyber-physical system,” in *Proc. SoutheastCon*, 2020, pp. 1–8.

[164] G. Sabaliauskaite and A. P. Mathur, “Aligning cyber-physical system safety and security,” in *Complex Systems Design & Management Asia*. Cham, Switzerland: Springer, 2015, pp. 41–53.

[165] Q. Liu, T. Han, and N. Ansari, “Learning-assisted secure end-to-end network slicing for cyber-physical systems,” *IEEE Netw.*, vol. 34, no. 3, pp. 37–43, May/Jun. 2020.

[166] S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber–physical system security for the electric power grid,” *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[167] H. L. Gawand, A. Bhattacharjee, and K. Roy, “Securing a cyber physical system in nuclear power plants using least square approximation and computational geometric approach,” *Nucl. Eng. Technol.*, vol. 49, no. 3, pp. 484–494, 2017.

[168] R. Gottumukkala, R. Merchant, A. Tauzin, K. Leon, A. Roche, and P. Darby, “Cyber-physical system security of vehicle charging stations,” in *Proc. IEEE Green Technol. Conf. (GreenTech)*, 2019, pp. 1–5.

[169] A. Chattopadhyay and K.-Y. Lam, “Security of autonomous vehicle as a cyber-physical system,” in *Proc. 7th Int. Symp. Embedded Comput. Syst. Design (ISED)*, 2017, pp. 1–6.

[170] O. A. Topal et al., “A physical layer security framework for cognitive cyber-physical systems,” *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 32–39, Aug. 2020.

[171] Y. Kim, V. Kolesnikov, and M. Thottan, "Resilient end-to-end message protection for cyber-physical system communications," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2478–2487, Jul. 2018.

[172] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surveys*, vol. 46, no. 4, pp. 1–29, 2014.

[173] C. S. Wickramasinghe, D. L. Marino, K. Amarasinghe, and M. Manic, "Generalization of deep learning for cyber-physical system security: A survey," in *Proc. 44th Annu. Conf. IEEE Ind. Electron. Soc.*, 2018, pp. 745–751.

[174] S. Huang, C.-J. Zhou, S.-H. Yang, and Y.-Q. Qin, "Cyber-physical system security for networked industrial processes," *Int. J. Autom. Comput.*, vol. 12, no. 6, pp. 567–578, 2015.

[175] W. Yu et al., "A framework for cyber-physical system security situation awareness," in *Principles of Cyber-Physical Systems: An Interdisciplinary Approach*. Cambridge, U.K.: Cambridge Univ. Press, 2020, p. 229.

[176] H. Yoo and T. Shon, "Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture," *Future Gener. Comput. Syst.*, vol. 61, pp. 128–136, Aug. 2016.

[177] C. Alcaraz and J. Lopez, "Secure interoperability in cyber-physical systems," in *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications*. Hershey, PA, USA: IGI Global, 2020, pp. 521–542.

[178] A. Aigner and A. Khelil, "An effective semantic security metric for industrial cyber-physical systems," in *Proc. IEEE Conf. Ind. Cyberphys. Syst. (ICPS)*, vol. 1, 2020, pp. 87–92.

[179] G. Kavallieratos, S. K. Katsikas, and V. Gkioulos, "Towards a cyber-physical range," in *Proc. 5th Cyber-Phys. Syst. Security Workshop*, 2019, pp. 25–34.

[180] T. Kumar et al., "BlockEdge: Blockchain-edge framework for industrial IoT networks," *IEEE Access*, vol. 8, pp. 154166–154185, 2020.

[181] G. Lacava et al., "Current research issues on Cyber security in robotics," 2020.

[182] F. Maggi, D. Quarta, M. Pogliani, M. Polino, A. M. Zanchettin, and S. Zanero, *Rogue Robots: Testing the Limits of An Industrial Robot's Security*, Trend Micro, Politecnico di Milano, Milan, Italy, 2017.

[183] G. McGraw, "Software security," *IEEE Security Privacy*, vol. 2, no. 2, pp. 80–83, Mar./Apr. 2004.

[184] R. White, M. Quigley, and H. I. Christensen, "SROS: Securing ROS over the wire, in the graph, and through the kernel," in *Proc. Humanoids Workshop Towards Humanoid Robots OS*, 2016, pp. 1–2.

[185] B. Dieber, S. Kacianka, S. Rass, and P. Schartner, "Application-level security for ROS-based applications," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst.*, 2016, pp. 4477–4482.

[186] T. Bai, J. Wang, Y. Ren, and L. Hanzo, "Energy-efficient computation offloading for secure UAV-edge-computing systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 6074–6087, Jun. 2019.

[187] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[188] C. Zhong, J. Yao, and J. Xu, "Secure UAV communication with cooperative jamming and trajectory control," *IEEE Commun. Lett.*, vol. 23, no. 2, pp. 286–289, Feb. 2019.

[189] A. Li, Q. Wu, and R. Zhang, "UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 181–184, Feb. 2019.

[190] M. Iqbal and S. Lim, "Legal and ethical implications of GPS vulnerabilities," *Int. J. Commun. Law Policy*, vol. 3, p. 178, Jan. 2008.

[191] S. Warner and R. Johnston, "GPS spoofing countermeasures," *Homeland Security J.*, vol. 25, pp. 19–27, Jan. 2003.

[192] S. Vitturi, C. Zunino, and T. Sauter, "Industrial communication systems and their future challenges: Next-generation Ethernet, IIoT, and 5G," *Proc. IEEE*, vol. 107, no. 6, pp. 944–961, Jun. 2019.

[193] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proc. IEEE*, vol. 95, no. 1, pp. 138–162, Jan. 2007.

[194] J.-D. Decotignie, "Ethernet-based real-time and industrial communications," *Proc. IEEE*, vol. 93, no. 6, pp. 1102–1117, Jun. 2005.

[195] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[196] R. Fujdiak et al., "Security in low-power wide-area networks: State-of-the-art and development toward the 5G," in *LPWAN Technologies for IoT and M2M Applications*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 373–396.

[197] D. Singh, G. Tripathi, and A. J. Jara, "A survey of Internet-of-Things: Future vision, architecture, challenges and services," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 287–292.

[198] S. K. Sharma and X. Wang, "Live data analytics with collaborative edge and cloud processing in wireless IoT networks," *IEEE Access*, vol. 5, pp. 4621–4635, 2017.

[199] J. G. Andrews et al., "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[200] X. Ge, S. Tu, G. Mao, C. Wang, and T. Han, "5G ultra-dense cellular networks," *IEEE Wireless Commun.*, vol. 23, no. 1, pp. 72–79, Feb. 2016.

[201] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, and P. Popovski, "Five disruptive technology directions for 5G," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 74–80, Feb. 2014.

[202] Z. Pi and F. Khan, "An introduction to millimeter-wave mobile broadband systems," *IEEE Commun. Mag.*, vol. 49, no. 6, pp. 101–107, Jun. 2011.

[203] J. G. Herrera and J. F. Botero, "Resource allocation in NFV: A comprehensive survey," *IEEE Trans. Netw. Service Manag.*, vol. 13, no. 3, pp. 518–532, Sep. 2016.

[204] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1657–1681, 3rd Quart., 2017.

[205] I. Farris, T. Taleb, Y. Khettab, and J. Song, "A survey on emerging SDN and NFV security mechanisms for IoT systems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 812–837, 1st Quart., 2019.

[206] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin, "Securing massive MIMO at the physical layer," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, 2015, pp. 272–280.

[207] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3880–3900, Jul. 2016.

[208] F. Kretschmer, S. Friedl, A. Lechler, and A. Verl, "Communication extension for cloud-based machine control of simulated robot processes," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, 2016, pp. 54–58.

[209] *Industrial Control System Security-Top 10 Threats and Countermeasures 2016*, Fed. Office Inf. Security, Bonn, Germany, 2019.

[210] W. A. Khan, L. Wisniewski, D. Lang, and J. Jasperneite, "Analysis of the requirements for offering industrie 4.0 applications as a cloud service," in *Proc. IEEE 26th Int. Symp. Ind. Electron. (ISIE)*, 2017, pp. 1181–1188.

[211] *Communications Requirements of Smart Grid Technologies*, U.S. Dept. Energy, Washington, DC, USA, pp. 1–69, 2010.

[212] B. Huang, X. Cheng, Y. Cao, and L. Zhang, "Lightweight hardware based secure authentication scheme for fog computing," in *Proc. IEEE/ACM Symp. Edge Comput. (SEC)*, 2018, pp. 433–439.

[213] C. Pu and T. Song, "Hatchetman attack: A denial of service attack against routing in low power and lossy networks," in *Proc. 5th IEEE Int. Conf. Cyber Security Cloud Comput. (CSCloud)/Proc. 4th IEEE Int. Conf. Edge Comput. Scalable Cloud (EdgeCom)*, 2018, pp. 12–17.

[214] Y. Niu, J. Zhang, A. Wang, and C. Chen, "An efficient collision power attack on AES encryption in edge computing," *IEEE Access*, vol. 7, pp. 18734–18748, 2019.

[215] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: State of the art and challenges," *Proc. IEEE*, vol. 107, no. 8, pp. 1608–1631, Aug. 2019.

[216] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, Jul. 2017.

[217] J. Wu, M. Dong, K. Ota, J. Li, W. Yang, and M. Wang, "Fog-computing-enabled cognitive network function virtualization for an information-centric future Internet," *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 48–54, Jul. 2019.

[218] J. Ni, K. Zhang, and A. V. Vasilakos, "Security and privacy for mobile edge caching: Challenges and solutions," *IEEE Wireless Commun.*, vol. 28, no. 3, pp. 77–83, Jun. 2021.

[219] R. Tourani, S. Misra, T. Mick, and G. Panwar, "Security, privacy, and access control in information-centric networking: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 566–600, 1st Quart., 2018.

[220] A. C. Baktir, A. Ozgovde, and C. Ersoy, "How can edge computing benefit from software-defined networking: A survey, use cases, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2359–2391, 4th Quart., 2017.

[221] S. Misra and N. Saha, "Detour: Dynamic task offloading in software-defined fog for IoT applications," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 5, pp. 1159–1166, May 2019.

[222] J. Wang, Y. Tan, J. Liu, and Y. Zhang, "Topology poisoning attack in SDN-enabled vehicular edge network," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9563–9574, Oct. 2020.

[223] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges," *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X16305635

[224] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards deep learning models resistant to adversarial attacks," 2017, *arXiv:1706.06083*.

[225] Q. Wu, W. Mei, and R. Zhang, "Safeguarding wireless network with UAVs: A physical layer security perspective," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 12–18, Oct. 2019.

[226] M. Arthur, "Detecting signal spoofing and jamming attacks in UAV networks using a lightweight IDS," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst.*, 2019, pp. 1–5.

[227] E. Ranyal and K. Jain, "Unmanned aerial vehicle's vulnerability to GPS spoofing a review," *J. Indian Soc. Remote Sens.*, vol. 49, pp. 585–591, Nov. 2020.

[228] A. Kerns, D. Shepard, J. Bhatti, and T. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *J. Field Robot.*, vol. 31, no. 4, pp. 617–636, 2014.

[229] Q. Wu, Y. Zeng, and R. Zhang, "Joint trajectory and communication design for multi-UAV enabled wireless networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 2109–2121, Mar. 2018.

[230] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV communications via joint trajectory and power control," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 1376–1389, Feb. 2019.

[231] M. Edrich and R. Schmalenberger, "Combined DSSS/FHSS approach to interference rejection and navigation support in UAV communications and control," in *Proc. IEEE 7th Int. Symp. Spread Spectr. Techn. Appl.*, 2002, pp. 687–691.

[232] B. W. O'Hanloon, M. L. Psiaki, T. E. Humphreys, and J. A. Bhatti, "Real-time spoofing detection using correlation between two civil GPSreceiver," in *Proc. ION GNSS Meeting*, 2012, pp. 3584–3590.

[233] K. Jansen, M. Shäfer, D. Moser, V. Lenders, C. Pöpper, and J. Schmitt, "Crowd-GPS-sec: Leveraging crowd sourcing to detect and localize GPS spoofing attacks," in *Proc. IEEE Symp. Security Privacy (SP)*, 2018, pp. 1018–1031.

[234] A. Eldosouky, A. Ferdowski, and W. Saad, "Drones in distress: A game-theoretic countermeasure for protecting UAVs against GPS spoofing," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2840–2854, Apr. 2020.

[235] C. Schwaiger and T. Sauter, "Security strategies for field area networks," in *Proc. IEEE 28th Annu. Conf. Ind. Electron. Soc.*, vol. 4, 2002, pp. 2915–2920.

[236] C. S. Park and H. M. Nam, "Security architecture and protocols for secure MQTT-SN," *IEEE Access*, vol. 8, pp. 226422–226436, 2020.

[237] P. Marcon et al., "Communication technology for industry 4.0," in *Proc. Progr. Electromagn. Res. Symp.*, 2017, pp. 1694–1697.

[238] F. Chen, Y. Huo, J. Zhu, and D. Fan, "A review on the study on MQTT security challenge," in *Proc. IEEE Int. Conf. Smart Cloud (SmartCloud)*, 2020, pp. 128–133.

[239] S. Vinoski, "Advanced message queuing protocol," *IEEE Internet Comput.*, vol. 10, no. 6, pp. 87–89, Nov./Dec. 2006.

[240] *Advanced Message Queuing Protocol Specification V0-9-1: Protocol Specification*, Cisco Syst., San Jose, CA, USA, 2008.

[241] A. Chaudhary, S. K. Peddoju, and K. Kadarla, "Study of Internet-of-Things Messaging protocols used for exchanging data with external sources," in *Proc. IEEE 14th Int. Conf. Mobile Ad Hoc Sens. Syst. (MASS)*, 2017, pp. 666–671.

[242] L. Coetzee, D. Oosthuizen, and B. Mkhize, "An analysis of CoAP as transport in an Internet of Things environment," in *Proc. IST-Afr. Week Conf. (IST-Afr.)*, 2018, pp. 1–7.

[243] C. Bormann, A. P. Castellani, and Z. Shelby, "CoAP: An application protocol for billions of tiny Internet nodes," *IEEE Internet Comput.*, vol. 16, no. 2, pp. 62–67, Mar./Apr. 2012.

[244] T. P. Raptis, A. Passarella, and M. Conti, "A survey on industrial Internet with ISA100 wireless," *IEEE Access*, vol. 8, pp. 157177–157196, 2020.

[245] T. Gebremichael et al., "Security and privacy in the Industrial Internet of Things: Current standards and future challenges," *IEEE Access*, vol. 8, pp. 152351–152366, 2020.

[246] X. Vilajosana, T. Watteyne, T. Chang, M. Vučinić, S. Duquennoy, and P. Thubert, "IETF 6TiSCH: A tutorial," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 595–615, 1st Quart., 2020.

[247] K. O. Akpinar and I. Ozcelik, "Analysis of machine learning methods in EtherCAT-based anomaly detection," *IEEE Access*, vol. 7, pp. 184365–184374, 2019.

[248] K.-H. Niemann, "IT security extensions for PROFINET," in *Proc. IEEE 17th Int. Conf. Ind. Inform. (INDIN)*, vol. 1, 2019, pp. 407–412.

[249] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things architecture, possible applications and key challenges," in *Proc. 10th Int. Conf. Front. Inf. Technol.*, Dec. 2012, pp. 257–260.

[250] J. A. Stankovic, "Research directions for the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, Feb. 2014.

[251] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128610001568

[252] A.-A. A. Boulogeorgos, P. D. Diamantoulakis, and G. K. Karagiannidis, "Low power wide area networks (LPWANs) for Internet of Things (IoT) applications: Research challenges and future trends," 2016, *arXiv:1611.07449v1*.

[253] F. Shaikh, E. Bou-Harb, N. Neshenko, A. P. Wright, and N. Ghani, "Internet of Malicious Things: Correlating active and passive measurements for inferring and characterizing Internet-scale unsolicited IoT devices," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 170–177, Sep. 2018.

[254] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018.

[255] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.

[256] M. I. Ayadi, F. Z. Saadaoui, A. Maizatc, M. Ouzzif, and C. Mahmoudi, "Deep learning for packet forwarding with an application for real time IoT," in *Proc. Int. Conf. Sel. Topics Mobile Wireless Netw. (MoWNeT)*, 2018, pp. 142–148.

[257] T. Alladi, V. Chamola, B. Sikdar, and K. R. Choo, "Consumer IoT: Security vulnerability case studies and solutions," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 17–25, Mar. 2020.

[258] J. C. Zuniga and B. Ponsard, "Sigfox system description," LPWAN@ IETF97, Internet Draft-draft-zuniga-lpwan-sigfox-system-description-01, IETF, Nov. 2016.

[259] C. Alcaraz, G. Bernieri, F. Pascucci, J. Lopez, and R. Setola, "Covert channels-based stealth attacks in industry 4.0," *IEEE Syst. J.*, vol. 13, no. 4, pp. 3980–3988, Dec. 2019.

[260] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[261] J. Song et al., "WirelessHART: Applying wireless technology in real-time industrial process control," in *Proc. IEEE Real-Time Embedded Technol. Appl. Symp.*, 2008, pp. 377–386.

[262] S. Petersen and S. Carlsen, "WirelessHART versus ISA100.11a: The format war hits the factory floor," *IEEE Ind. Electron. Mag.*, vol. 5, no. 4, pp. 23–34, Dec. 2011.

[263] T. Kumar, A. Braeken, V. Ramani, I. Ahmad, E. Harjula, and M. Ylianttila, "SEC-BlockEdge: Security threats in blockchain-edge based industrial IoT networks," in *Proc. 11th Int. Workshop Resilient Netw. Design Model. (RNDM)*, 2019, pp. 1–7.

[264] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019.

[265] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Bus. Inf. Syst. Eng.*, vol. 59, no. 3, pp. 183–187, 2017.

[266] J. Granjal, E. Monteiro, and J. Sá Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.

[267] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[268] J. Sengupta, S. Ruj, and S. D. Bit, "A secure fog-based architecture for industrial Internet of Things and industry 4.0," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2316–2324, Apr. 2021.

[269] J. Li, Y. Liu, T. Chen, Z. Xiao, Z. Li, and J. Wang, "Adversarial attacks and defenses on cyber–physical systems: A survey," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5103–5115, Jun. 2020.

[270] M. A. Akheel et al., "Vulnerability assessment and analysis of SCADA and foundation fieldbus on industrial control system (ICS) networks: A literature review," *IUP J. Comput. Sci.*, vol. 17, no. 2, pp. 34–65, 2023.

[271] *Industry 4.0—Cybersecurity Challenges and Recommendations*, ENISA, Athens, Greece, 2019.

[272] *Good Practices for Security of IoT—Secure Software Development Lifecycle*, ENISA, Athens, Greece, 2019.

[273] A. Ghafouri, Y. Vorobeychik, and X. Koutsoukos, "Adversarial regression for detecting attacks in cyber-physical systems," 2018, *arXiv:1804.11022*.

[274] J. Li, J. Y. Lee, Y. Yang, J. S. Sun, and K. Tomsovic, "ConAML: Constrained adversarial machine learning for cyber-physical systems," 2020, *arXiv:2003.05631*.

[275] P. F. de Araujo-Filho, G. Kaddoum, D. R. Campelo, A. G. Santos, D. Macêdo, and C. Zanchettin, "Intrusion detection for cyber–physical systems using generative adversarial networks in fog environment," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6247–6256, Apr. 2021.

[276] B. Brenner et al., "Better safe than sorry: Risk management based on a safety-augmented network intrusion detection system," *IEEE Open J. Ind. Electron. Soc.*, vol. 4, pp. 287–303, 2023.

[277] *Industrial Communication Networks—Network and System Security—Part 2-1: Establishing an Industrial Automation and Control System Security Program*, IEC Standard 62443-2-1, 2010.

[278] A. Evesti, J. Suomalainen, and E. Ovaska, "Architecture and knowledge-driven self-adaptive security in smart space," *Computers*, vol. 2, no. 1, pp. 34–66, 2013.

[279] Y. Shan, Y. Yao, T. Zhao, and W. Yang, "NeuPot: A neural network-based honeypot for detecting cyber threats in industrial control systems," *IEEE Trans. Ind. Informat.*, vol. 19, no. 10, pp. 10512–10522, Oct. 2023.

[280] S. Sourav and B. Chen, "Exposing hidden attackers in industrial control systems using micro-distortions," *IEEE Trans. Smart Grid*, early access, Aug. 7, 2023, doi: 10.1109/TSG.2023.3300710.

[281] H. Zhu, M. Liu, C. Fang, R. Deng, and P. Cheng, "Detection-performance tradeoff for watermarking in industrial control systems," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 2780–2793, 2023.

[282] B. Genge and C. Siaterlis, "An experimental study on the impact of network segmentation to the resilience of physical processes," in *Proc. Int. Conf. Res. Netw.*, 2012, pp. 121–134.

[283] V. M. Vilches et al., "Introducing the robot security framework (RSF), a standardized methodology to perform security assessments in robotics," in *Proc. Symp. Blockchain Robot. Syst.*, 2018, pp. 1–19.

[284] F. Callegati, W. Cerroni, and M. Ramilli, "Man-in-the-middle attack to the HTTPS protocol," *IEEE Security Privacy*, vol. 7, no. 1, pp. 78–81, Jan./Feb. 2009.

[285] A. Baitha and S. Vinod, "Session hijacking and prevention technique," *Int. J. Eng. Technol.*, vol. 7, p. 193, Mar. 2018.

[286] S. Belikovetsky, M. Yampolskiy, J. Toh, and Y. Elovici, "dr0wned—Cyber-physical attack with additive manufacturing," in *Proc. 11th USENIX Workshop Offensive Technol.*, 2017, pp. 1–16.

[287] D. Portugal, S. Pereira, and M. S. Couceiro, "The role of security in human-robot shared environments: A case study in ROS-based surveillance robots," in *Proc. 26th IEEE Int. Symp. Robot Human Interactive Commun. (RO-MAN)*, 2017, pp. 981–986.

[288] M. Mukhandi, D. Portugal, S. Pereira, and M. S. Couceiro, "A novel solution for securing robot communications based on the MQTT protocol and ROS," in *Proc. IEEE/SICE Int. Symp. Syst. Integr. (SII)*, 2019, pp. 608–613.

[289] J. Lambrecht, M. Chemnitz, and J. Krüger, "Control layer for multi-vendor industrial robot interaction providing integration of supervisory process control and multifunctional control units," in *Proc. IEEE Conf. Technol. Pract. Robot Appl.*, 2011, pp. 115–120.

[290] "Fast DDS documentation." eProsima. Accessed: Oct. 2023. [Online]. Available: https://fast-dds.docs.eprosima.com/en/latest/

[291] V. DiLuoffo, W. Michalson, and B. Sunar, "Robot operating system 2: The need for a holistic security approach to robotic architectures," *Int. J. Adv. Robot. Syst.*, vol. 15, no. 3, May 2018, Art. no. 1729881418770011.

[292] Q. Ge and F. Chen, "Strategies for implementing SSL on embedded system," in *Proc. Int. Seminar Future BioMedical Inf. Eng.*, 2008, pp. 457–460.

[293] R. Toris, C. Shue, and S. Chernova, "Message authentication codes for secure remote non-native client connections to ROS enabled robots," in *Proc. IEEE Int. Conf. Technol. Pract. Robot Appl.*, 2014, pp. 1–6.

[294] Y. Maruyama, S. Kato, and T. Azumi, "Exploring the performance of ROS2," in *Proc. 13th Int. Conf. Embedded Softw.*, 2016, pp. 1–10.

[295] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and privacy in the medical Internet of Things: A review," *Security Commun. Netw.*, vol. 2018, Mar. 2018, Art. no. 5978636.

[296] Y. Xu, G. Wang, J. Ren, and Y. Zhang, "An adaptive and configurable protection framework against android privilege escalation threats," *Future Gener. Comput. Syst.*, vol. 92, pp. 210–224, Mar. 2019.

[297] K. Kenthapadi, I. Mironov, and A. G. Thakurta, "Privacy-preserving data mining in industry," in *Proc. 12th ACM Int. Conf. Web Search Data Min.*, 2019, pp. 840–841.

[298] S. Potluri, C. Diedrich, and G. K. R. Sangala, "Identifying false data injection attacks in industrial control systems using artificial neural networks," in *Proc. 22nd IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, 2017, pp. 1–8.

[299] I. H. Sarker, A. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: An overview from machine learning perspective," *J. Big Data*, vol. 7, no. 1, pp. 1–29, 2020.

[300] A. De, M. N. I. Khan, K. Nagarajan, and S. Ghosh, "HarTBleed: Using hardware trojans for data leakage exploits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 4, pp. 968–979, Apr. 2020.

[301] P. W. Khan and Y. Byun, "A blockchain-based secure image encryption scheme for the Industrial Internet of Things," *Entropy*, vol. 22, no. 2, p. 175, 2020.

[302] G. Qiu, C. Wang, S. Luo, and W. Xu, "A dual dynamic key chaotic encryption system for industrial cyber-physical systems," *IEICE Electron. Exp.*, vol. 17, no. 24, 2020, Art. no. 20200389.

[303] K. Zhang, J. Long, X. Wang, H.-N. Dai, K. Liang, and M. Imran, "Lightweight searchable encryption protocol for Industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 4248–4259, Jun. 2021.

[304] S. Wang, J. Wan, D. Zhang, D. Li, and C. Zhang, "Towards smart factory for industry 4.0: A self-organized multi-agent system with big data based feedback and coordination," *Comput. Netw.*, vol. 101, pp. 158–168, Jun. 2016.

[305] T. M. Fernandez-Carames, O. Blanco-Novoa, I. Froiz-Miguez, and P. Fraga-Lamas, "Towards an autonomous industry 4.0 warehouse: A UAV and blockchain-based system for inventory and traceability applications in big data-driven supply chain management," *Sensors*, vol. 19, no. 10, p. 2394, 2019.

[306] S. H. Alsamhi, E. Curry, A. Hawbani, S. Kumar, U. U. Hassan, and N. S. Rajput, "DataSpace in the sky: A novel Decentralized framework to secure drones data sharing in B5G for industry 4.0 toward industry 5.0," Preprints, 2023. [Online]. Available: https://doi.org/10.20944/preprints202305.0529.v1

[307] G. Li, K. Ota, M. Dong, J. Wu, and J. Li, "DeSVig: Decentralized swift vigilance against adversarial attacks in industrial artificial intelligence systems," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3267–3277, May 2020.

[308] G. Li, J. Wu, S. Li, W. Yang, and C. Li, "Multitentacle federated learning over software-defined Industrial Internet of Things against adaptive poisoning attacks," *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 1260–1269, Feb. 2023.

[309] A. Qayyum, M. Usama, J. Qadir, and A. Al-Fuqaha, "Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 998–1026, 2nd Quart., 2020.

[310] A. N. Bhagoji, S. Chakraborty, S. Calo, and P. Mittal, "Model poisoning attacks in federated learning," presented at Workshop Security Mach. Learn. (SecML) Collocated 32nd Conf. Neural Inf. Process. Syst. (NeurIPS), 2018.

[311] R. Balakrishnan, M. Akdeniz, S. Dhakal, and N. Himayat, "Resource management and fairness for federated learning over wireless edge networks," in *Proc. IEEE 21st Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, 2020, pp. 1–5.

[312] J. Zhang, B. Chen, X. Cheng, H. T. T. Binh, and S. Yu, "PoisonGAN: Generative poisoning attacks against federated learning in edge computing systems," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3310–3322, Mar. 2021.

[313] J. Chi et al., "Privacy partition: A privacy-preserving framework for deep neural networks in edge networks," in *Proc. IEEE/ACM Symp. Edge Comput. (SEC)*, 2018, pp. 378–380.

[314] D. Kaur, S. Uslu, K. J. Rittichier, and A. Durresi, "Trustworthy artificial intelligence: A review," *ACM Comput. Surveys*, vol. 55, no. 2, pp. 1–38, 2022.

[315] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?" *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 41–49, Sep. 2018.

[316] J. Chen, X. Gao, R. Deng, Y. He, C. Fang, and P. Cheng, "Generating adversarial examples against machine learning-based intrusion detector in industrial control systems," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 3, pp. 1810–1825, May/Jun. 2022.

[317] Y. Li, Y. Song, L. Jia, S. Gao, Q. Li, and M. Qiu, "Intelligent fault diagnosis by fusing domain adversarial training and maximum mean discrepancy via ensemble learning," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2833–2841, Apr. 2021.

[318] M. Lecuyer, V. Atlidakis, R. Geambasu, D. Hsu, and S. Jana, "Certified robustness to adversarial examples with differential privacy," in *Proc. IEEE Symp. Security Privacy (SP)*, 2019, pp. 656–672.

[319] B. Esmaeili, A. Azmoodeh, A. Dehghantanha, H. Karimipour, B. Zolfaghari, and M. Hammoudeh, "IIoT deep malware threat hunting: From adversarial example detection to adversarial scenario detection," *IEEE Trans. Ind. Informat.*, vol. 18, no. 12, pp. 8477–8486, Dec. 2022.

[320] Z. Yan, J. Wu, G. Li, S. Li, and M. Guizani, "Deep neural backdoor in semi-supervised learning: Threats and countermeasures," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4827–4842, 2021.

[321] B. Hou et al., "Mitigating the backdoor attack by federated filters for industrial IoT applications," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3562–3571, May 2022.

[322] Y. Li, X. Lyu, N. Koren, L. Lyu, B. Li, and X. Ma, "Neural attention distillation: Erasing backdoor triggers from deep neural networks," 2021, *arXiv:2101.05930*.

[323] J. Orlosky, K. Kiyokawa, and H. Takemura, "Virtual and augmented reality on the 5G highway," *J. Inf. Process.*, vol. 25, pp. 133–141, Feb. 2017.

[324] S. Li, P. Zheng, and L. Zheng, "An AR-assisted deep learning-based approach for automatic inspection of aviation connectors," *IEEE Trans. Ind. Informat.*, vol. 17, no. 3, pp. 1721–1731, Mar. 2021.

[325] F. Pires, A. Cachada, J. Barbosa, A. P. Moreira, and P. Leitão, "Digital twin in industry 4.0: Technologies, applications and challenges," in *Proc. IEEE 17th Int. Conf. Ind. Inform. (INDIN)*, vol. 1, 2019, pp. 721–726.

[326] F. Roesner, T. Kohno, and D. Molnar, "Security and privacy for augmented reality systems," *Commun. ACM*, vol. 57, no. 4, pp. 88–96, 2014.

[327] T. M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez-Albela, and M. Vilar-Montesinos, "A fog computing and cloudlet based augmented reality system for the industry 4.0 shipyard," *Sensors*, vol. 18, no. 6, p. 1798, 2018.

[328] M. Fiorentino, S. Debernardis, A. E. Uva, and G. Monno, "Augmented reality text style readability with see-through head-mounted displays in industrial context," *Presence*, vol. 22, no. 2, pp. 171–190, 2013.

[329] J. A. De Guzman, K. Thilakarathna, and A. Seneviratne, "Security and privacy approaches in mixed reality: A literature survey," *ACM Comput. Surveys*, vol. 52, no. 6, pp. 1–37, 2019.

[330] M. Schneider, J. Rambach, and D. Stricker, "Augmented reality based on edge computing using the example of remote live support," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, 2017, pp. 1277–1282.

[331] M. Khamis, F. Alt, M. Hassib, E. von Zezschwitz, R. Hasholzner, and A. Bulling, "Gazetouchpass: Multimodal authentication using gaze and touch on mobile devices," in *Proc. CHI Conf. Extended Abstracts Human Factors Comput. Syst.*, 2016, pp. 2156–2164.

[332] M. Khamis, M. Hassib, E. V. Zezschwitz, A. Bulling, and F. Alt, "GazeTouchPIN: Protecting sensitive data on mobile devices using secure multimodal authentication," in *Proc. 19th ACM Int. Conf. Multimodal Interact.*, 2017, pp. 446–450.

[333] K. Lebeck, K. Ruth, T. Kohno, and F. Roesner, "Securing augmented reality output," in *Proc. IEEE Symp. Security Privacy (SP)*, 2017, pp. 320–337.

[334] S. Ahn, M. Gorlatova, P. Naghizadeh, M. Chiang, and P. Mittal, "Adaptive fog-based output security for augmented reality," in *Proc. Morning Workshop Virtual Reality Augmented Real. Netw.*, 2018, pp. 1–6.

[335] A. Aryan and S. Singh, "Securing location privacy in augmented reality," in *Proc. 5th Int. Conf. Ind. Inf. Syst.*, 2010, pp. 172–176.

[336] S. Barra, K.-K. R. Choo, M. Nappi, A. Castiglione, F. Narducci, and R. Ranjan, "Biometrics-as-a-service: Cloud-based technology, systems, and applications," *IEEE Cloud Comput.*, vol. 5, no. 4, pp. 33–37, Jul./Aug. 2018.

[337] Z. Feng, P. Zhou, Q. Wang, and W. Qi, "A dual-layer zero trust architecture for 5G industry MEC applications access control," in *Proc. IEEE 5th Int. Conf. Electron. Inf. Commun. Technol. (ICEICT)*, 2022, pp. 100–105.

[338] T. H. Szymanski, "The "Cyber security via determinism" paradigm for a quantum safe zero trust deterministic Internet of Things (IoT)," *IEEE Access*, vol. 10, pp. 45893–45930, 2022.

[339] T. M. Fernandez-Carames and P. Fraga-Lamas, "A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories," *IEEE Access*, vol. 7, pp. 45201–45218, 2019.

[340] L. Bader et al., "Blockchain-based privacy preservation for supply chains supporting lightweight multi-hop information accountability," *Inf. Process. Manage.*, vol. 58, no. 3, 2021, Art. no. 102529.

[341] M. Saad et al., "Exploring the attack surface of blockchain: A systematic overview," 2019, *arXiv:1904.03487*.

[342] B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, "A blockchain-based architecture for collaborative DDoS mitigation with smart contracts," in *Proc. IFIP Int. Conf. Auton. Infrastructure, Manage. Security*, 2017, pp. 16–29.

[343] S. Zhang and J. Lee, "Double-spending with a Sybil attack in the bitcoin decentralized network," *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5715–5722, Oct. 2019.

[344] A. Malik, S. Gautam, S. Abidin, and B. Bhushan, "Blockchain technology-future of IoT: Including structure, limitations and various possible attacks," in *Proc. 2nd Int. Conf. Intell. Comput., Instrum. Control Technol. (ICICICT)*, vol. 1, 2019, pp. 1100–1104.

[345] K. M. Khan, J. Arshad, and M. M. Khan, "Empirical analysis of transaction malleability within blockchain-based e-voting," *Comput. Security*, vol. 100, Jan. 2021, Art. no. 102081.

[346] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Appl. Sci.*, vol. 9, no. 9, p. 1788, 2019.

[347] H. Lee, M. Shin, K. S. Kim, Y. Kang, and J. Kim, "Recipient-oriented transaction for preventing double spending attacks in private blockchain," in *Proc. 15th Annu. IEEE Int. Conf. Sens., Commun., Netw. (SECON)*, 2018, pp. 1–2.

[348] M. Kędziora, P. Kozłowski, M. Szczepanik, and P. Jóźwiak, "Analysis of blockchain selfish mining attacks," in *Proc. Int. Conf. Inf. Syst. Archit. Technol.*, 2019, pp. 231–240.

[349] L. Wei, J. Wu, C. Long, and Y. Lin, "The convergence of IoE and blockchain: Security challenges," *IT Prof.*, vol. 21, no. 5, pp. 26–32, 2019.

[350] J. Moubarak, E. Filiol, and M. Chamoun, "On blockchain security and relevant attacks," in *Proc. IEEE Middle East North Afr. Commun. Conf. (MENACOMM)*, 2018, pp. 1–6.

[351] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (SoK)," in *Proc. Int. Conf. Princ. Security Trust*, 2017, pp. 164–186.

[352] P. Kumar, R. Kumar, G. P. Gupta, and R. Tripathi, "A distributed framework for detecting DDoS attacks in smart contract-based blockchain-IoT systems by leveraging fog computing," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 6, 2020, Art. no. e4112.

[353] P. Racsko, "Blockchain and democracy," *Soc. Econ.*, vol. 41, no. 3, pp. 353–369, 2019.

[354] K. M. Khan, J. Arshad, and M. M. Khan, "Simulation of transaction malleability attack for blockchain-based e-Voting," *Comput. Electr. Eng.*, vol. 83, May 2020, Art. no. 106583.

[355] M. Bastiaan, "Preventing the 51%-attack: A stochastic analysis of two phase proof of work in bitcoin," 2015. [Online]. Available: http://referaat.cs.utwente.nl/Conf./22/paper/7473/preventingthe-51-attack-a-stochasticanalysis-oftwo-phase-proof-of-work-bitcoin.pdf

[356] J. Bae and H. Lim, "Random mining group selection to prevent 51% attacks on bitcoin," in *Proc. 48th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops (DSN-W)*, 2018, pp. 81–82.

[357] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, 2014.

[358] T. T. Huynh, T. D. Nguyen, and H. Tan, "A survey on security and privacy issues of blockchain technology," in *Proc. Int. Conf. Syst. Sci. Eng. (ICSSE)*, 2019, pp. 362–367.

[359] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in *Proc. ACM Conf. Comput. Commun. Security*, 2012, pp. 906–917.

[360] M. Saad, L. Njilla, C. Kamhoua, and A. Mohaisen, "Countering selfish mining in blockchains," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, 2019, pp. 360–364.

[361] E. Heilman, "One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner," in *Proc. Int. Conf. Financ. Cryptograph. Data Security*, 2014, pp. 161–162.

[362] S. Solat and M. Potop-Butucaru, "Zeroblock: Timestamp-free prevention of block-withholding attack in bitcoin," 2016, *arXiv:1605.02435*.

[363] K. Nicolas, Y. Wang, and G. C. Giakos, "Comprehensive overview of selfish mining and double spending attack countermeasures," in *Proc. IEEE 40th Sarnoff Symp.*, 2019, pp. 1–6.

[364] L. Zhu et al., "Research on the security of blockchain data: A survey," 2018, *arXiv:1812.02009*.

[365] J. Liu and Z. Liu, "A survey on security verification of blockchain smart contracts," *IEEE Access*, vol. 7, pp. 77894–77904, 2019.

[366] S. Sayeed, H. Marco-Gisbert, and T. Caira, "Smart contract: Attacks and protections," *IEEE Access*, vol. 8, pp. 24416–24427, 2020.

[367] "SmartM2M; IoT standards landscape and future evolutions," ETSI, Sophia Antipolis, France, Rep. ETSI TR 103 375, 2016.

[368] "Federal office for information security of Germany." Accessed: Oct. 2023. [Online]. Available: https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html

[369] "The national institute of standards and technology (NIST)." Accessed: Oct. 2023. [Online]. Available: https://www.nist.gov/

[370] *Framework for Improving Critical Infrastructure Cybersecurity*, Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, 2018.

[371] F. Heylighen and C. Joslyn, "What is systems theory?" in *Cambridge Dictionary of Philosophy*. Cambridge, U.K.: Cambridge Univ. Press, 1992.

[372] F. Heylighen and C. Joslyn, "Cybernetics and second-order cybernetics," in *Encyclopedia of Physical Science Technology*, vol. 4. New York, NY, USA: Academic, 2001, pp. 155–170.

[373] S. Umpleby, "The role of cybernetics in security policy," *Cybern. Human Knowing*, vol. 21, no. 4, pp. 79–82, 2014.

[374] M. D. Adams, S. D. Hitefield, B. Hoy, M. C. Fowler, and T. C. Clancy, "Application of cybernetics and control theory for a new paradigm in cybersecurity," 2013, *arXiv:1311.0257.*

[375] P. Bhosale, W. Kastner, and T. Sauter, "A centralised or distributed risk assessment using asset administration shell," in *Proc. 26th IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, 2021, pp. 1–4.

[376] K. Thoma, *Resilien-Tech. 'Resilience by Design: A Strategy for the Technology Issues of the Future*, Acatech Nat. Acad. Sci. Eng., Washington, DC, USA, 2014.

[377] P. Bhosale, W. Kastner, and T. Sauter, "Automating safety and security risk assessment in industrial control systems: Challenges and constraints," in *Proc. IEEE 27th Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, 2022, pp. 1–4.

[378] "Secure use of ICS-specific apps." Federal Office for Information Security of Germany. 2019. [Online]. Available: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_103E.pdf;jsessionid=41581140AC58885CA2EE045E9EE9DB70.2_cid500?__blob=publicationFile&v=2

[379] "Managing information security risk," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. NIST SP 800-39, Mar. 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

[380] *Industrial Communication Networks—Network and System Security*, IEC Standard 62443, Jul. 2009. [Online]. Available: https://webstore.iec.ch/publication/7029

[381] *Information Technology—Security Techniques—Evaluation Criteria for IT Security*, ISO/IEC Standard 15408, Dec. 2009. [Online]. Available: https://www.iso.org/standard/50341.html

[382] *Information Technology—Security Techniques—Information Security Management Systems*, ISO/IEC Standard 27000:2018, Feb. 2018. [Online]. Available: https://www.iso.org/standard/73906.html

[383] *IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities*, Int. Atomic Energy Agency (IAEA), Vienna, Austria, 2011. [Online]. Available: https://www.iaea.org/publications/8691/computer-security-at-nuclear-facilities

[384] *Nuclear Power Plants—Instrumentation, Control and Electrical Power Systems—Cybersecurity Requirements*, IEC 62645:2019, Nov. 2019. [Online]. Available: https://webstore.iec.ch/publication/32904

[385] *Nuclear Power Plants—Instrumentation, Control and Electrical Power Systems—Security Controls*, IEC 63096:2020, Oct. 2020. [Online]. Available: https://webstore.iec.ch/publication/32900

[386] "6G research visions, No. 8: 6G white paper on edge intelligence." Jun. 2020. [Online]. Available: https://www.6gchannel.com/items/6g-white-paper-edge-intelligence/

[387] S. Wang et al., "Adaptive federated learning in resource constrained edge computing systems," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 6, pp. 1205–1221, Jun. 2019.

[388] J. Wang, J. Hu, G. Min, W. Zhan, Q. Ni, and N. Georgalas, "Computation offloading in multi-access edge computing using a deep sequential model based on reinforcement learning," *IEEE Commun. Mag.*, vol. 57, no. 5, pp. 64–69, May 2019.

[389] N. Shan, X. Cui, and Z. Gao, "'DRL + FL': An intelligent resource allocation model based on deep reinforcement learning for mobile edge computing," *Comput. Commun.*, vol. 160, pp. 14–24, Jul. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S014036641932122X

[390] S. Autolitano and A. Pawlowska, "Europe's quest for digital sovereignty: GAIA-X as a case study," 2021. [Online]. Available: https://www.jstor.org/stable/resrep309401963

[391] *Reference Architecture Model, Version 3.0*. Berlin, Germany: Int. Data Spaces Assoc., 2019.

[392] M. Huber, S. Wessel, G. Brost, and N. Menz, "Building trust in data spaces," in *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage*, B. Otto, M. ten Hompel, and S. Wrobel, Eds. Cham, Switzerland: Springer Nat., 2022, pp. 147–164.

[393] A. Braud, G. Fromentoux, B. Radier, and O. Le Grand, "The road to European digital sovereignty with Gaia-X and IDSA," *IEEE Netw.*, vol. 35, no. 2, pp. 4–5, Mar./Apr. 2021.

[394] B. Otto, M. Ten Hompel, and S. Wrobel, *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage*. Cham, Switzerland: Springer Nat., 2022.

[395] M. de la Cámara, F. Sáenz, J. Calvo-Manzano, and M. Arcilla, "Security by design factors for developing and evaluating secure software," in *Proc. Iberian Conf. Inf. Syst. Technol. (CISTI)*, 2015, pp. 1–6.

[396] H. Alemzadeh, D. Cheng, X. Li, T. Kesavadas, Z. Kalbarczyk, and R. Iyer, "Targeted attacks on teleoperated surgical robots: Dynamic model-based detection and mitigation," in *Proc. Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw.*, 2016, pp. 395–406.

[397] A. Jovicic, J. Li, and T. Richardson, "Visible light communication: Opportunities, challenges and the path to market," *IEEE Commun. Mag.*, vol. 51, no. 12, pp. 26–32, Dec. 2013.

[398] A. Mostafa and L. Lampe, "Physical-layer security for MISO visible light communication channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 9, pp. 1806–1818, Sep. 2015.

[399] C. M. Snipp, "What does data sovereignty imply: What does it look like," in *Indigenous Data Sovereignty: Toward an Agenda*. Acton, ACT, Australia: Aust. Nat. Univ. Press, Nov. 2016, pp. 39–55.

[400] "The International Data Spaces." Accessed: Oct. 2023. [Online]. Available: https://www.internationaldataspaces.org/

[401] B. Otto, M. T. Hompel, and S. Wrobel, *International Data Spaces*. Heidelberg, Germany: Springer, 2019, pp. 109–128. [Online]. Available: https://doi.org/10.1007/978-3-662-58134-6_8

[402] R. Parasuraman, T. B. Sheridan, and C. D. Wickens, "A model for types and levels of human interaction with automation," *IEEE Trans. Syst., Man Cybern., A: Syst. Humans*, vol. 30, no. 3, pp. 286–297, May 2000.

[403] M. G. Kibria, K. Nguyen, G. P. Villardi, K. Ishizu, and F. Kojima, "Next generation new radio small cell enhancement: Architectural options, functionality and performance aspects," *IEEE Wireless Commun.*, vol. 25, no. 4, pp. 120–128, Aug. 2018.

[404] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Towards software defined cognitive networking," in *Proc. 7th Int. Conf. New Technol., Mobility Security (NTMS)*, Jul. 2015, pp. 1–5.

[405] R. Mahajan, D. Wetherall, and T. Anderson, "Understanding BGP misconfiguration," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 32, no. 4, pp. 3–16, 2002.

[406] "SDN security considerations in the data center." Open Networking Foundation. Oct. 2013. [Online]. Available: https://www.opennetworking.org/sdn-resources/sdn-library

[407] H. Hamed and E. Al-Shaer, "Taxonomy of conflicts in network security policies," *IEEE Commun. Mag.*, vol. 44, no. 3, pp. 134–141, Mar. 2006.

[408] A. Wool, "A quantitative study of firewall configuration errors," *Computer*, vol. 37, no. 6, pp. 62–67, Jun. 2004.

[409] N. G. Nayak, F. Dürr, and K. Rothermel, "Software-defined environment for reconfigurable manufacturing systems," in *Proc. 5th Int. Conf. Internet Things (IOT)*, 2015, pp. 122–129.

IJAZ AHMAD (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in wireless communications from the University of Oulu, Finland, in 2012 and 2018, respectively. He is currently working with the VTT Technical Research Centre of Finland, and is an Adjunct Professor with the University of Oulu. He has been a Visiting Scientist with the Technical University of Vienna, Austria, in 2019, and Aalto University, Finland, in 2018. His research interests include cybersecurity, security of 5G/6G, and the applications of machine learning in wireless networks. He is the recipient of several awards, including the Nokia Foundation, Tauno Tönning, and Jorma Ollila Grant Awards, and the VTT Research Excellence Awards in 2020 and 2021. Furthermore, he has received two best paper awards at IEEE conferences.

FELIPE RODRIGUEZ received the M.Sc. degree in communications engineering from Aalto University in 2020. Previously, he worked as a Research Scientist with the Technical Research Centre of Finland (VTT), where he participated in national and international research projects related to 5G and 6G communication networks. He is currently working as a Specification Engineer with Nokia. His interests include security and automation of 5G and 6G networks, as well as wireless communications.

TANESH KUMAR (Member, IEEE) received the B.E. degree in computer engineering from the National University of Sciences and Technology (E&ME), Pakistan, in 2012, the M.Sc. degree in computer science from South Asian University, New Delhi, India, in 2014, and the D.Sc. degree in communications engineering from the University of Oulu, Finland, in 2016, where he is currently working as a Postdoctoral Researcher with the Centre for Wireless Communications. He has coauthored over 40 peer-reviewed scientific articles. His current research interests include security, privacy, and trust in the IoT networks, 5G/6G security, edge computing, DLTs/blockchain, and medical ICT.

JANI SUOMALAINEN received the M.Sc. (Tech.) degree from the Lappeenranta University of Technology, Finland, and the D.Sc. (Tech.) degree from Aalto University, Finland. Since 2000, he has been with the VTT Technical Research Centre of Finland, Espoo, where he is a Senior Scientist. He is specialized on cybersecurity and has been involved in these topics in various international joint projects and customer projects. He has researched smart security applications, security interoperability, as well as developed ML-based threat detection and security situation awareness systems for software-defined mobile networks. His research interests include adaptive and learning security solutions for dynamic and heterogeneous network environments.

SENTHIL KUMAR JAGATHEESAPERUMAL received the B.E. degree from Madurai Kamaraj University, India, in 2003, the Postgraduate degree from Anna University, Chennai, India, in 2005, and the Ph.D. degree in information and communication engineering from Anna University, Chennai, India, in 2017. He is currently working as an Associate Professor (Senior Grade) with the Department of Electronics and Communication Engineering, Mepco Schlenk Engineering College, Sivakasi, India. He received two funded research projects from National Instruments, USA, each worth USD 50 000 in 2015 and 2016, respectively. He also received another funded research project from IITM-RUTAG in 2017 worth Rs. 3.97 Lakhs. During his career, he has published various papers in international journals and conferences. His area of research includes robotics, Internet of Things, embedded systems, and wireless communication. He is a Life Member of IETE and ISTE.

STEFAN WALTER received the Doctoral degree from the University of Lapland, Finland, where he specialized in sustainable development and adaptation to changing conditions using socio-cybernetic principles. He is a Senior Scientist in VTT's Intelligent Supply Chains and Logistics Research Team, which focuses on agile and sustainable supply chain responses through cognitive technologies. He has worked in several management and consultancy positions in the logistics industry and has occupied full-time and adjunct teaching positions. He has been involved in a large variety of research projects and published numerous conference and journal articles. His research interests include the digitalization of supply chains, business and economic development, sustainability, and cybernetics. He is a reviewer for several international journals.

MUHAMMAD ZEESHAN ASGHAR received the M.Sc. and Ph.D. degrees in software engineering from the University of Oulu, Finland, in 2010 and 2018, respectively. He is currently working with Enfuce as a Software Developer. His current research interests include remote healthcare, assisted living, augmented reality, and virtual reality.

GAOLEI LI (Member, IEEE) received the B.S. degree in electronic information engineering from Sichuan University, Chengdu, China, and the Ph.D. degree in cyber security from Shanghai Jiao Tong University, Shanghai, China. From October 2018 to September 2019, he visited the Muroran Institution of Technology, Muroran, Japan, supported by the China Scholarship Council Program. He is currently an Assistant Professor with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University. His research interests include network security, adversarial machine learning, and privacy computing. He has received Best Paper Awards from the IEEE ComSoc CSIM Committee, Chinese Association for Cryptologic Research, and Student Travel Grant Award for IEEE Globecom. He is a TPC Member of AAAI 2023, IEEE ICC 2018–2022, and a Reviewer of IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, and IEEE Transactions on Cognitive Communications and Networking.

NIKOLAOS PAPAKONSTANTINOU received the Doctoral degree in information technology in automation from Aalto University, Finland, in 2012. He is an Electrical and Computer Engineer with the University of Patras, Greece, in 2008. He is a docent in the field of information technologies in industrial applications in 2020. He is leading the Applied cybersecurity Team, VTT Technical Research Centre of Finland. VTT is a large non-profit research organization with both commercial and public research activities. The interests of the team include security training, device testing, security design/architectures, platform security as well as holistic security assessment of industrial systems, and other critical infrastructure. His personal interests focus on early resilience (safety/security) engineering for complex sociotechnical systems.

MIKA YLIANTTILA (Senior Member, IEEE) received the M.Sc., Dr.Sc., and eMBA degrees. He is a Full Professor with the Centre for Wireless Communications—Networks and Systems Research Unit, Faculty of Information Technology and Electrical Engineering, University of Oulu, Finland. He is the Director of Communications Engineering Doctoral Degree Program and leads NetSEC (Network security, trust, and privacy) Research Group which studies and develops secure, scalable and resource-efficient techniques for 5G and beyond 5G, and IoT systems. He has coauthored more than 200 international peer-reviewed articles. He is an Associate Editor of IEEE Transactions on Information Forensics and Security.

JYRKI HUUSKO received the degree in theoretical physics with minor subjects in information technology and mathematics from the University of Oulu. He is working with the VTT Technical Research Centre of Finland as a Research Team Leader. His current research topics include future autonomic networks and services, transport protocols and multimedia delivery optimization, cross-layer communication design in heterogeneous wireless and mobile networks, cross-layer communication aided network mobility, and multiaccess.

THILO SAUTER (Fellow, IEEE) received the Ph.D. degree in electrical engineering from TU Wien, Vienna, Austria, in 1999. He was the Founding Director of the Department for Integrated Sensor Systems, University for Continuing Education Krems, Wiener Neustadt, Austria. He is currently a Professor of Automation Technology with TU Wien. He is author of more than 350 scientific publications and has held leading positions in renowned IEEE conferences. Moreover, he has been involved in the standardization of industrial communications for more than 25 years. His expertise and research interests include embedded systems and integrated circuit design, smart sensors, and automation and sensor networks with a focus on real-time, security, interconnection, and integration issues relevant to cyber–physical systems and the Internet of Things in various application domains, such as industrial and building automation, smart manufacturing, or smart grids. He is a Senior AdCom Member of the IEEE Industrial Electronics Society.

ERKKI HARJULA (Member, IEEE) received the D.Sc. degree in communications engineering from the University of Oulu, Finland, in 2016, where he is currently a Tenure-track Assistant Professor with the Centre for Wireless Communications. In the University of Oulu, he was with the Center for Internet Excellence, from 2013 to 2015, and the MediaTeam Research Group from 2000 to 2014. He visited Columbia University, New York, NY, USA, from 2008 to 2009, as a Researcher. He is a coauthor of over 80 international peer-reviewed scientific articles on mobile and IoT systems, edge computing, distributed systems, and energy efficiency.