IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 27 September 2024, accepted 13 October 2024, date of publication 17 October 2024, date of current version 8 November 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3482987

TOPICAL REVIEW

Leveraging Machine Learning for Cybersecurity Resilience in Industry 4.0: Challenges and Future Directions

JIA YU[1], ALEXEY V. SHVETSOV[2,3,4], AND SAEED HAMOOD ALSAMHI[5,6]

[1]School of Computer and Information Engineering, Luoyang Institute of Science and Technology, Luoyang 471023, China
[2]Department of Road Transport and Car Service Operations, North-Eastern Federal University, 677000 Yakutsk, Russia
[3]Engineering Center, Togliatti State University, 445020 Tolyatti, Russia
[4]Department of Transport Engineering and Technology, RUDN University, 117198 Moscow, Russia
[5]Department of Electrical Engineering, IBB University, Ibb, Yemen
[6]Department of Computer Science and Engineering, College of Informatics, Korea University, Seongbuk-gu, Seoul 02841, Republic of Korea

Corresponding author: Jia Yu (jia.yu@lit.edu.cn)

This work was supported in part by China Scholarship Council under Grant 202008410014, and in part by the Science and Technology Breakthrough Project of Henan Science and Technology Department under Grant 232102210065.

ABSTRACT Industry 4.0, where the convergence of digital technology impacts industrial operations and processes, is characterized by cybersecurity resilience. Therefore, in Industry 4.0, Machine Learning (ML) approaches offer enormous potential for strengthening cyber defenses, guaranteeing resistance against cyber attacks, and improving cyber resilience. One of the most significant trends is the rise of ML in cybersecurity. ML's ability to analyze vast amounts of data and detect threats that human operators will miss positions it as a crucial tool in the cybersecurity arsenal. This survey offers a comprehensive overview and examines how ML supports facets of cybersecurity, including risk evaluation, incident response sharing threat intelligence, intrusion detection, and safeguarding ML models from attacks. This survey discusses existing techniques' benefits and drawbacks, identifies emerging trends, and proposes research directions by scrutinizing current frameworks, case studies, and methodologies. Furthermore, we discuss several topics, including predictive risk assessment approaches, collaborative threat intelligence sharing platforms, ML-driven intrusion detection models, automated incident response strategies, and techniques for mitigating manipulations in ML models. Furthermore, the survey identifies the applications of language models in enhancing cybersecurity resilience. This article intends to offer an in-depth look at the advancements by drawing on knowledge from academic disciplines. Moreover, the survey aims to inspire concepts and strategies for bolstering cyber resilience in Industry 4.0 environments.

INDEX TERMS ML, cybersecurity, Industry 4.0, cyber resilience, intrusion detection, adversarial attacks.

I. INTRODUCTION

Industry 4.0 represents the advancement of processes, through the integration of cyber systems, IoT devices, and advanced automation technologies [1], [2], [3], [4], [5]. There are several techniques are used for improving the performance in Industry 4.0 applications such as blockchain, federated learning, digital twins, drones, and B5G networks [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18]. The Industry 4.0 era brings about cybersecurity challenges such as increased vulnerability to cyber-attacks and potential disruptions despite its promises of improved production and efficiency [19], [20], [21]. As a result, prioritizing cyber resilience and recovering from intrusions is crucial. Machine Learning (ML) is essential to Industry 4.0 success because it improves cyber resilience by quickly detecting anomalies and modifying defenses [22]. Due to Industry 4.0's interconnectedness, organizations are vulnerable to supply chain assaults and malware [23], [24], [25], [26], [27]. Furthermore, the fusion of IT and OT

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

environments blurs security boundaries making cybersecurity management more complex [28]. As a result, industrial companies encounter challenges, in safeguarding data protecting infrastructure, and ensuring operational continuity amidst evolving cyber threats [29]. In addition to following legal and regulatory requirements, important investments include IoT, ML-integrated security solutions as shown in Figure.1, and remote work security. Zero-trust platforms and next-generation firewalls are important examples of technology. This technological change also presents new difficulties for leaders. Technologically savvy leaders are crucial.

In the applications of Industry 4.0, ML methods such, as reinforcement learning, supervised learning, and unsupervised learning offer means to strengthen cyber resilience [30], [31], [32], [33]. Elements like selecting features ensuring data quality and constructing models could impact the efficacy of cybersecurity solutions driven by machine learning [35]. Support Vector Machines (SVMs) and neural networks are two anomaly detection approaches used by machine learning-powered intrusion detection systems to identify possible cyber threats and behaviors [36]. These systems analyze network traffic, system logs, and other data telemetry to detect deviations from behavior and trigger alerts. Predictive analytics are used in ML-based risk assessment methodologies to quantify cybersecurity risks and prioritize mitigation strategies [37]. By examining event data and contextual information ML models can identify risks assess their potential impacts and recommend actions to mitigate risk exposure [38].

Automated incident response solutions incorporate ML algorithms for faster threat detection, analysis, and remediation processes [39]. The systems leverage ML for tasks such as malware analysis, threat investigation, and timely response actions across IT environments. Using ML-powered threat intelligence systems makes gathering, standardizing, and linking threat data from origins simpler. The platforms help in finding risks sharing information and collaborating on strategy development among companies [40], [41]. Attacks, from adversaries pose a threat to the effectiveness and reliability of machine learning models creating a challenge, for cybersecurity solutions based on machine learning [42], [43]. The strategy to mitigate attacks involves implementing training methods identifying instances and encouraging model diversity.

A. RELATED SURVEYS

Research on the security and cybersecurity of Industry 4.0 has been limited [44], [45]. In [44] reviewed various works on anomaly detection for network traffic across various applications, including wireless sensor networks, IoT, high-performance computing, ICSs, and SDNs. The authors emphasized the need for improvement in anomaly detection, focusing on aspects such as detection rate, process complexity, false alarm rates, and real-time detection. They also highlighted the need for more research on anomaly detection for IoT systems. [45] conducted a survey on cybersecurity in Indistury 4.0 to address this gap. They presented a benchmark framework for analyzing cyber threats to industrial equipment and provided the latest countermeasures to safeguard IIoT infrastructure. however, the authors of [46] and [47] focused on cyber resilience. [46] conducted a systematic literature review of cyber resilience frameworks. They categorized these frameworks as either strategic or operational based on their impact on decision-making, the types of attacks they addressed, their methodologies, and the organization's location using them. This effort resulted in an informative overview of the current status of cyber resilience, pinpointing research gaps and emphasizing commonalities and synergies among different frameworks. While, [47] examined the cutting-edge methods for enhancing CPS resilience, encompassing various strategies aimed at reinforcing resilience through redundancy, fault tolerance, and security enhancements.

Early implementations of ML in cybersecurity primarily targeted anomaly detection and signature-based identification of known threats [35]. Advances in ML and intense learning have created more resilient and adaptive cybersecurity measures [48]. ML-powered threat detection systems utilize behavior analysis, anomaly detection, and pattern recognition methods to detect potential security breaches in real-time [49]. Innovations in adversarial ML have produced ML models capable of withstanding evasion techniques cybercriminals use [50]. ML-driven automated incident response systems can dramatically shorten response times, reducing the effects of cyberattacks [51]. Additionally, Edge ML platforms facilitate the deployment of lightweight, efficient security mechanisms to safeguard devices on the network edge [52]. ML in cybersecurity presents significant opportunities for mitigating cyber threats and protecting digital assets [53]. ML technologies are transforming the cybersecurity landscape, advancing areas such as threat detection, incident response, and the protection of IoT and edge devices. Despite these advancements, overcoming adversarial attacks and addressing ethical concerns is critical to fully harnessing ML's potential in this domain. By continuing research, fostering collaboration, and driving innovation, ML-powered cybersecurity solutions can adapt to the dynamic threat landscape and effectively safeguard digital ecosystems [54].

B. MOTIVATIONS AND CONTRIBUTIONS

The rapid advancement of Industry 4.0 technology has brought changes to processes enhancing connectivity, productivity, and efficiency. However along, with these advancements comes a rise in cybersecurity risks stemming from attack routes and vulnerabilities in systems and IoT devices. Industrial processes have been completely transformed by the quick development of Industry 4.0 technology, which has increased connectivity, productivity, and efficiency. However, while these developments occur, there is also a noticeable increase in cybersecurity risks due to new attack routes

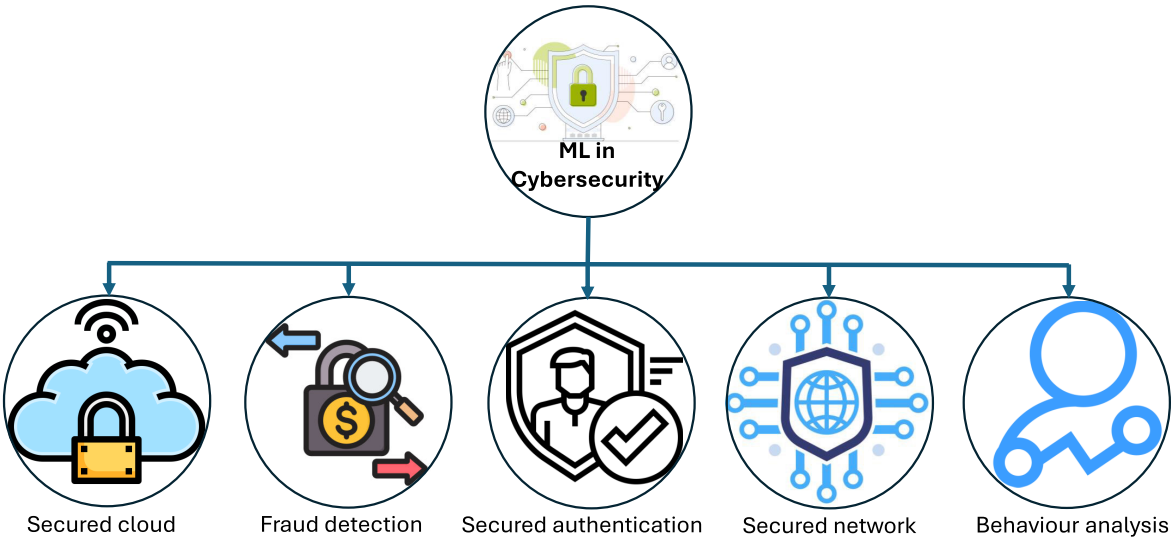

FIGURE 1. ML in cybersecurity.

and vulnerabilities in networked systems and IoT devices. Existing literature often focuses on ML applications or cybersecurity challenges without exploring how ML can effectively address the complex nature of cyber threats in Industry 4.0 settings. ML has become a viable method for boosting cyber resilience by using data-driven insights to identify, assess, and quickly respond to cyber threats.

This survey delves into cybersecurity applications related to machine learning, within the context of Industry 4.0 such as evaluating risks responding to incidents sharing threat intelligence detecting intrusions, and safeguarding machine learning models against attacks. Despite the growing use of machine learning in cybersecurity, there is a need to understand better how machine learning and cyber resilience interact within Industry 4.0 environments. Previous research has tended to concentrate on cybersecurity concerns or machine learning applications. does not provide a thorough examination of how machine learning may be used to counteract the complex cyber threats that characterize Industry 4.0. By shedding light on how machine learning-driven cybersecurity solutions improve cyber resilience in Industry 4.0, our study seeks to close this knowledge gap. We discuss the benefits and disadvantages of techniques in machine learning identify emerging trends and propose areas for development to address pressing challenges, in this critical domain. This paper's contributions are outlined as follows:

1) This survey investigates how ML methods can improve cyber resilience by systematically assessing ML applications in solving cybersecurity concerns within Industry 4.0. We explore several areas including adversarial attack mitigation, threat intelligence sharing, incident response, intrusion detection, and risk assessment, providing insights into the benefits and drawbacks of various ML techniques.
2) We emphasize the necessity of approaching ML-based cybersecurity solutions with a more integrated and comprehensive approach. Furthermore, we highlight the directions and challenges to improve the field of ML-driven cyber resilience in the environment of Industry 4.0.

C. PAPAER STRUCTURE

The rest of the paper is organized as follows. Section II discusses cybersecurity Challenges in Industry 4.0, while ML for cyber resilience is discussed in Section III. Section IV highlights ML applications in cyber resilience and challenges and future trends are discussed in section V. Finally, the paper is concluded in Section VI.

II. MACHINE LEARNING TECHNIQUES FOR VULNERABILITY ANALYSIS

Vulnerability research is a crucial step in cybersecurity, especially when considering Industry 4.0 and finding and fixing flaws in intricate systems. Vulnerability analysis is more accurate and efficient when using ML approaches [55], [56], [57]. This section thoroughly summarizes the several machine learning methods used in vulnerability assessments, emphasizing their uses, benefits, and drawbacks.

A. SUPERVISED LEARNING

By using labeled data to train models, the supervised learning technique helps them discover patterns and correlations that may be used to find weaknesses. In this area, algorithms like logistic regression, support vector machines, and neural networks are frequently used. For example, past vulnerability data may train supervised learning models using known patterns and features to anticipate possible future vulnerabilities [58]. When enough labeled data is available, supervised learning's main benefit is its capacity to provide precise predictions. However, it needs a significant quantity of labeled data to reach high performance, and it can have trouble identifying new or undiscovered vulnerabilities [59].

TABLE 1. Comparison of related surveys.

Ref.	Focus Area	ML Techniques Evaluated	Industry 4.0 Context	Traditional IT Cybersecurity Context	Key Contributions
[49] (2024)	General overview of ML applications in cybersecurity	Supervised Learning, Unsupervised Learning, Reinforcement Learning	Limited mention of Industry 4.0, primarily IT focus	Comprehensive evaluation of IT systems' security	Offers a broad review of ML techniques for general cybersecurity
[130] (2023)	Focused on AI and ML in IIoT security	Neural Networks, Reinforcement Learning	Strong focus on IIoT and industrial systems	Briefly touches on traditional IT systems	Specific focus on Industry 4.0, particularly IIoT and cyber-physical systems
[131] (2023)	Intrusion detection across various sectors	Decision Trees, Random Forests, Support Vector Machines	Focuses minimally on Industry 4.0	Comprehensive analysis of intrusion detection for IT systems	In-depth focus on ML for intrusion detection techniques, but lacks Industry 4.0 focus
[129] (2023)	Applied ML in cybersecurity detect and automate cyber threat responses	various ML techniques	some applications		cybersecurity and techniques to introducing the enhancing cyber security threat
This work	ML techniques specifically for Industry 4.0 cybersecurity	Supervised, Unsupervised, Semi-supervised Learning, Neural Networks, Reinforcement Learning	Strong focus on Industry 4.0, including IIoT and industrial control systems	Comparatively less focus on traditional IT cybersecurity	1. Extensive evaluation of ML for cyber resilience in Industry 4.0 2. Emphasis on IIoT, interconnected systems 3. Analysis of ML techniques for intrusion detection, risk assessment, incident response, and threat intelligence in Industry 4.0

B. UNSUPERVISED LEARNING

Conversely, unsupervised learning does not require labeled data. Instead, it uses its algorithm to find patterns and abnormalities in the data. Data analysis methods like clustering and dimensionality reduction are employed to find possible vulnerabilities in the data that do not match the usual patterns seen in the training set [60]. Unsupervised learning, for instance, might assist in spotting odd patterns in system behavior or network traffic that can point to vulnerabilities that have not yet been discovered. Unsupervised learning can help identify new vulnerabilities, but it frequently has significant false favorable rates and may need to be carefully adjusted to prevent misclassifications [61].

C. SEMI-SUPERVISED LEARNING

With a smaller pool of labeled data and a larger pool of unlabeled data, semi-supervised learning integrates aspects of supervised and unsupervised learning. This strategy is beneficial when there is a dearth of labeled data but a surplus of unlabeled data. Semi-supervised learning models can enhance their performance in vulnerability analysis tasks by utilizing both kinds of data [62]. By combining large amounts of unlabeled data from several sources with sparsely labeled vulnerability data, this method may be used to improve risk assessment models. Although semi-supervised learning models have several benefits, their effectiveness mostly depends on the caliber of the labeled data, and domain-specific modifications may be necessary [63].

D. REINFORCEMENT LEARNING

With Reinforcement Learning (RL), models may be trained to make decisions by interacting with their surroundings and getting feedback on what they do. Adaptive solutions for locating and addressing vulnerabilities in dynamic systems may be created using reinforcement learning in the context of vulnerability analysis [64]. For example, reinforcement learning algorithms learn from fresh data and can modify their tactics to tackle new threats. The flexibility RL can adjust to shifting conditions and develop over time strengthens it. To develop practical answers, RL can be computationally demanding and may need a thorough investigation of the action space [65].

III. CYBERSECURITY CHALLENGES IN INDUSTRY 4.0

The amount of applications and required data has grown significantly in recent years due to the Internet of Things (IoT) applications rising progress. Furthermore, there is a growing need for real-time data processing and analysis [66]. Industry 4.0 and IoT device convergence have ushered in a new era of sophisticated connectivity and data-driven decision-making. The security threats linked to IoT devices are data breaches, cyberattack vulnerabilities, privacy issues, and a lack of established security measures. Industry 4.0 becomes possible targets for malevolent activity if the dangers are not addressed. The amount of applications and required data has grown significantly in recent years due to IoT applications' rising progress. Furthermore, there is a growing need for real-time data processing and analysis [66]. Industry 4.0 and IoT device convergence have ushered in a new era of sophisticated connectivity and data-driven decision-making.

However, because the primary dangers to industrial processes are now closely linked to the vulnerabilities associated with networked IoT devices, this integration also poses serious security issues. The security threats connected to IoT are data breaches, privacy issues, cyberattack vulnerabilities, and a lack of established security measures. The procedures and systems of Industry 4.0 become possible targets for malevolent activity if these dangers are not addressed [67]. These challenges arise from the dispersed architecture and high data throughput of edge computing, which prevents the complete deployment of typical information security protection techniques employed in Industry 4.0 for the protection of such information inside it. Two significant aspects that demonstrate the complexity based on Industry 4.0 have been chosen from earlier research [68], [69] and are covered in different tables to address the aforementioned problems. Industry 4.0, which integrates cyber-physical systems, IoT devices, and enhanced automation, is a paradigm change in industrial operations [1], [72]. Because digital

technologies are linked, Industry 4.0 presents significant cybersecurity risks in addition to its many benefits, such as enhanced efficiency and flexibility [73]. The dynamic threat landscape, which presents severe hazards to sensitive data, vital infrastructure, and operational continuity, is one of the main obstacles [74].

Several critical trends define the evolving threat landscape within the context of Industry 4.0. First, the adoption of networked systems and the growth of IoT devices expand the attack surface available to cyber criminals. The gadgets, which can be anything from industrial robots to sensors and actuators, frequently have weak security protections, which leaves them open to hacking and other security flaws [75]. Furthermore, merging OT and IT systems blurs the lines between traditional security measures, opening up new attack avenues for cyberattacks. Threat actors, which comprise nation-states, criminal groups, and hacktivist groups, take advantage of weaknesses in industrial systems to accomplish a range of nefarious goals, including financial gain, espionage, and destruction.

Furthermore, the digitalization of industrial operations brings additional hazards related to data availability, integrity, and privacy. Industrial firms are more vulnerable to insider threats, ransomware attacks, and data breaches due to gathering and analyzing massive volumes of data from many sources. Furthermore, the use of third-party suppliers and cloud services, for data processing and storage can pose risks to the supply chain. In situations attackers may exploit vulnerabilities within the system to undermine and cause disturbances in operations [19]. To address these cybersecurity challenges businesses in the sector need to adopt an all-encompassing approach to managing risks. Safeguarding assets involves implementing security measures like intrusion detection systems, encryption protocols, and access controls. Additionally, companies should emphasize cybersecurity training for their employees. Promote a culture of security within the organization. Collaboration among enterprises, government entities, and educational institutions is essential, for sharing threat intelligence, best practices and resources to mitigate cyber risks effectively [74].

The increased attack surface brought about by the integration of various industrial components, such as sensors, actuators, controllers, and industrial robots, is one of the main cybersecurity problems [76]. Cyber attackers looking to penetrate and compromise vital infrastructure might use any of these components as an entry point. Furthermore, the merging of IT and operational technology (OT) blurs the boundaries between conventional security measures, creating new attack vectors for assaults. Cybercriminals make use of flaws in networked systems to disrupt operations, steal private data, or hurt people [77].

Furthermore, as IoT devices proliferate, the number of endpoints they introduce increases, increasing the danger of cybersecurity breaches due to either weak security features or improper configuration [78]. The gadgets, which can be anything from wearable technology and driverless cars to smart sensors and security cameras, frequently function in surroundings with low processing and memory capacity. Therefore, It could be vulnerable to a range of cyberattacks, such as denial-of-service (DoS) assaults, malware infections, and remote exploits [79]. In [70], the authors introduced an advanced adversarial method utilizing Generative Adversarial Networks (GANs) to effectively compromise malware classifiers, even without prior knowledge of the data or the system, a technique referred to as a black-box attack. Furthermore, the authors of [71] executed realistic adversarial attacks targeting network intrusion detection systems, which employ machine learning classifiers to detect botnet traffic. Their findings demonstrated the effectiveness of such attacks.

Additionally, because industrial systems are heterogeneous, managing cybersecurity becomes more difficult because enterprises must deal with various old and developing technologies, vendor-specific solutions, and proprietary protocols. Because of this complexity, it is challenging to apply standardized security controls and keep an eye on the whole attack surface [80]. Furthermore, the lengthy lifespan of industrial assets might provide difficulties for patch management and vulnerability remediation since updates and vendor support may be lost for outdated systems. Industrial firms must implement a multi-layered protection plan with proactive, investigative, and response measures to counter these cybersecurity threats. To safeguard critical assets and data, substantial access restrictions, network segmentation, encryption, and intrusion detection systems must be put in place [81]. Organizations should also prioritize cybersecurity awareness training for staff members and cultivate a security-conscious culture at all organizational levels [82]. In addition, sharing threat intelligence, best practices, and resources for reducing cyber risks requires cooperation between government agencies, cybersecurity experts, and industry players.

In cybersecurity, resilience pertains to the capacity of an entity to endure and bounce back from cyberattacks, disturbances, or malfunctions while preserving crucial operations and amenities. Resilience recognizes that breaches and events are unavoidable and aims to reduce their effect and duration, in contrast to traditional security approaches primarily focused on prevention and detection [83]. For several reasons, the significance of resilience in Industry 4.0 cannot be emphasized. First, because industrial systems are linked, a breach in one part might spread across the whole ecosystem, making them more vulnerable to cyberattacks. As a result, enterprises need to take a comprehensive strategy for resilience that considers the interdependencies and domino consequences of cyberattacks.

Second, because vital activities rely on digital technology, robust defensive systems are required to guarantee uninterrupted operation in the face of cyber-attacks [74]. Industrial process disruptions or downtime may seriously affect the economy, safety, and reputation, emphasizing the necessity

for solid resilience solutions. Furthermore, because cyber threats are dynamic and ever-changing, firms must quickly respond to new risks and vulnerabilities and adjust as needed. Resilient organizations can quickly resume regular operations by reducing the impact of cyberattacks and detecting and mitigating them in real-time [84]. Moreover, organizational, procedural, cultural, and technical factors are all included in the concept of resilience. A resilient cybersecurity posture requires effective incident response, crisis management, and communication mechanisms. Long-term success also depends on cultivating a resilient culture within the company, which is marked by awareness, cooperation, and constant progress [85].

The challenge in Industry 4.0 installations is the use of insecure connection methods. Resource economy precedes security in protocols like MQTT and CoAP, which frequently lack strong encryption or authentication mechanisms [120]. This puts IIoT devices at risk for data manipulation and interception, where bad actors can change or falsify essential data. IIoT devices are also more vulnerable due to their physical accessibility. The IIoT-related supply chain vulnerabilities additionally exacerbate the overall security concerns. Devices can be compromised by malicious actors at any point along the production, delivery, or maintenance process, resulting in complex supply chain assaults that are hard to identify [121]. These assaults have the potential to generate hidden vulnerabilities that linger long after they are deployed, which might eventually allow attackers to get access to systems. Moreover, special hazards are introduced by the IIoT systems' necessity for real-time operations. Cyberattack disruptions, such as Distributed Denial of Service (DDoS) assaults, can have dire repercussions very away, putting safety-critical systems in jeopardy or stopping industrial operations [122].

The availability and integrity of data are critical in IIoT situations because compromised data poses severe dangers to public safety. For instance, fabricated sensor data may lead to equipment failure, resulting in mishaps or environmental risks. Attackers frequently target the operational technologies in charge of managing physical processes to take advantage of these data integrity and safety concerns [123], [124], [125]. After an attacker gains access to an IIoT system, there are severe hazards from lateral movement and Advanced Persistent Threats (APTs). These enemies can travel laterally through the network, breaching vital control systems and carrying out well-planned operations that might have disastrous consequences [126]. Malware and ransomware are popular threat vectors in IIoT systems that can impede operations by encrypting important data or resulting in system outages [127], [128]. Table.2 summarises the unique vulnerabilities and attack vectors in IIoT deployment.

IV. ML FOR CYBER RESILIENCE

ML approaches are essential to enhancing cyber resilience because MLs offer automated threat identification, prediction, and real-time response. Understanding ML concepts is essential if you want to employ these techniques to fortify cybersecurity defenses in Industry 4.0 environments. Fundamentally, ML is a branch of Artificial Intelligence (AI) that concentrates on creating models and algorithms that can learn from data and make judgments or predictions without the need for explicit programming. supervised learning, unsupervised learning, and reinforcement learning are the three main categories into which ML approaches fall in the context of cybersecurity [87]. Using labeled data—each data point having a matching label or outcome—supervised learning entails training a model. By minimizing a predetermined loss function, such as mean squared error or cross-entropy loss, the model learns to map input data to output labels [88]. Table.3 illustrates the ML fundamentals for cyber resilience.

Using input features, data is categorized into predetermined groups, such as benign or malignant. Decision trees, logistic regression, and support vector machines (SVM) are examples of common categorization methods [89]. However, regression is the process of forecasting an output variable or continuous value from input information. Regression algorithms are used for tasks like evaluating the probability of a security event or forecasting the severity of cyber attacks [90]. Examples of these algorithms are linear regression and random forest regression. In contrast, unsupervised learning uses unlabeled data to train a model to find hidden structures, patterns, or anomalies. Unlike supervised learning, unsupervised learning algorithms seek to find underlying groupings or correlations in the data, which requires labeled data.

Clustering is assembling comparable data elements according to shared traits or attributes. Anomaly detection and identifying odd patterns in network traffic are two tasks for which clustering methods, such as k-means and hierarchical clustering, are employed [91]. While dimensionality Reduction Reducing the intricacy of high-dimensional data while maintaining its key characteristics is known as dimensionality reduction. For feature selection, visualization, and anomaly detection, dimensionality reduction methods like principal component analysis (PCA)and t-distributed stochastic neighbor embedding (t-SNE) are employed [92].

ML paradigm known as reinforcement learning teaches an agent how to interact with its surroundings by acting in a way that maximizes cumulative rewards or minimizes punishments. Although they are not frequently used directly in cybersecurity, reinforcement learning techniques can be used for automated incident triage, adaptive security policies, and dynamic threat response [93]. However, the benefits and limitations of ML are illustrated in Table.3 ML algorithms are a flexible means of improving cyber resilience through the automation of critical cybersecurity functions including incident response, intrusion detection, and risk assessment [49]. To successfully use ML algorithms to strengthen cybersecurity defenses in Industry 4.0 environments as shown

TABLE 2. Vulnerabilities and attack in industry 4.0.

Category	Description	Key vulnerabilities	Attack vectors
Device heterogeneity & Legacy systems	The diversity of devices, including legacy systems with outdated security measures, creates vulnerabilities.	Lack of standardization, outdated firmware, and insufficient patching.	Exploits of known vulnerabilities, malware targeting old systems.
Insecure communication protocols	IIoT protocols prioritize efficiency, often neglecting strong security, leading to data transmission risks.	Weak encryption, unsecured connections, and data interception risks.	Man-in-the-Middle (MitM) attacks, eavesdropping, and data tampering.
Physical Accessibility	IIoT devices are often located in physically insecure environments, making them prone to tampering or sabotage.	Physical tampering, unauthorized access, and device manipulation.	Physical attacks, tampering, insertion of malicious hardware.
Supply chain vulnerabilities	The supply chain can introduce vulnerabilities during the manufacturing, shipping, or installation of IIoT devices.	Hidden malware, backdoors [86], and compromised devices entering the network.	Supply chain attacks, hardware Trojan insertion, firmware tampering.
Real-time operational risks	Disruption of real-time operations in critical industrial processes can lead to system failures or safety risks.	Delays or disruptions in operational data, compromised control systems.	Ransomware, Denial-of-Service (DoS), process manipulation.
Data integrity & Safety Risks	Manipulation of sensor data or control commands can compromise safety-critical processes in industrial systems.	Falsified sensor data, unauthorized changes to control systems, and safety breaches.	Data integrity attacks, false data injection, system sabotage.
Lateral movement & APTs	Attackers can move laterally across IIoT networks, exploiting multiple points to target critical infrastructure.	Weak network segmentation, insecure access controls, unmonitored activity.	Advanced Persistent Threats (APTs), lateral movement, privilege escalation.
Common attack vectors	Attack methods specifically targeting IIoT systems' vulnerabilities.	Broad attack surface due to unpatched or vulnerable systems.	Malware, ransomware, insider threats, network-based attacks.

in Figure. 2, it is imperative to comprehend how these tasks might be applied to ML algorithms.

1) **Detecting intrusions:** Intrusion detection, which entails locating and reacting to illegal access or malicious activity within a network, frequently makes use of ML methods [94]. In order to categorize incoming traffic as benign or malicious, supervised learning techniques, such as support vector machines (SVMs), decision trees, and deep neural networks, can be trained on labeled datasets of normal and anomalous network traffic [95]. These algorithms look for trends that point to cyberattacks such as port scanning, denial-of-service (DoS) assaults, and malware infections by analyzing network packets, system logs, and other telemetry data [96]. Anomaly detection methods, such as autoencoders and isolation forests, can also be used to spot departures from the usual and set off alarms for possible intrusions [97]. ML-driven cybersecurity workflow for resilience in Industry 4.0 with addressing IIoT-specific threats through synthetic data generation,

TABLE 3. ML advantages and limitations for Cyber resilience.

ML Technique	Description	Advantages	Limitations
Supervised Learning	Utilizes labeled training data to learn patterns and make predictions. Commonly used in intrusion detection and malware classification tasks.	- Effective for detecting known patterns and attacks - Can be trained with labeled data	- Limited to detecting known patterns - Requires labeled training data
Unsupervised Learning	Learning patterns from unlabeled data and detect anomalies. Suitable for identifying unusual behavior in network traffic and system logs.	- Can detect novel or unknown patterns and anomalies - Does not require labeled training data	- Prone to high false positive rates - May struggle with imbalanced datasets
Semi-supervised Learning	Combines labeled and unlabeled data for training. Useful when labeled data is scarce but unlabeled data is abundant. Can be applied to risk assessment and threat detection tasks.	- Utilizes both labeled and unlabeled data - Can leverage small amounts of labeled data for training	- Performance may depend on the quality of labeled data - May require domain expertise for effective labeling
Reinforcement Learning	Learns to make decisions through trial and error, receiving feedback from the environment. Suitable for adaptive incident response strategies and dynamic cyber threat mitigation.	- Can learn optimal actions based on feedback from the environment - Well-suited for dynamic and adaptive environments	- Requires exploration of action space - May suffer from high computational complexity
Neural Networks	Models are inspired by the structure of the human brain, consisting of interconnected nodes (neurons) organized in layers. Can be applied to various cybersecurity tasks, including intrusion detection and malware classification.	- Capable of learning complex patterns and relationships - Versatile and suitable for various tasks in cybersecurity	- Requires large amounts of data and computational resources - May be prone to overfitting if not properly regularized
Decision Trees	Hierarchical tree-like structures that make decisions based on feature values. Easy to interpret and suitable for decision-making in risk assessment and incident response.	- Easy to interpret and visualize - Can handle both numerical and categorical data	- Prone to overfitting, especially with deep trees - Sensitive to small variations in data
Random Forests	Ensemble learning technique that combines multiple decision trees to improve accuracy and robustness. Effective for intrusion detection and classification tasks in cybersecurity.	- Ensemble learning improves generalization and robustness - Can handle large datasets with high dimensionality	- May be computationally expensive - Model interpretability decreases with the number of trees in the forest
Support Vector Machines	construct hyperplanes in a high-dimensional space to separate classes. Useful for detecting complex patterns in cybersecurity data and classifying network traffic.	- Effective for high-dimensional data and complex decision boundaries - Versatile with different kernel functions	- May require careful selection of kernel and hyperparameters - Limited interpretability of decision boundaries
Naive Bayes	Probabilistic classifier based on Bayes' theorem. Simple and fast, making it suitable for real-time intrusion detection and email filtering applications.	- Simple and fast to train and deploy - Performs well with small datasets and high-dimensional feature spaces	- Assumes independence between features, which may not hold in practice - Sensitivity to imbalanced class distributions and rare events

genetic algorithms for feature selection, and advanced ML-based detection mechanisms to enable real-time response and system hardening is shown in Figure.3. It outlines typical widespread cyber threats in business environments, such as malware insertion, data exfiltration, and denial of service (DoS). Essential machine learning methods are integrated into the core portion of the workflow, such as creating synthetic data to mimic attack situations, feature selection based on genetic algorithms to enhance the detection process, and ML-based detection models to spot abnormalities or assaults. The resilience mechanisms include system hardening, automatic incident response, and threat intelligence sharing, and they are all designed to preserve operational continuity and strengthen defenses against potential assaults.

2) **Evaluation of Risk:** ML algorithms are also utilized in risk assessment, wherein cybersecurity threats are ranked and quantified according to their likelihood and potential consequences [98]. Using contextual data and previous event data, supervised learning algorithms may be taught to create predictive models that forecast the likelihood of particular cyber threats materializing as well as any possible repercussions [99]. These models identify high-risk locations and suggest mitigation techniques by analyzing many risk variables, including organizational assets, threat intelligence, and vulnerabilities [100]. Moreover, new dangers may be recognized, and hidden patterns in data can be found using unsupervised learning approaches such as association rule mining and clustering [101]. Organizations may allocate resources more efficiently and prevent cyber threats by proactively incorporating ML-based risk assessment approaches into their decision-making processes [101].
3) **Reaction to an Incident:** In order to reduce the damage of cyberattacks, incident response, which entails real-time cyberattack detection, analysis, and mitigation, depends heavily on ML algorithms [103]. ML algorithms are used by automated incident response solutions to analyze malware, detect threats, and make decisions. To create models that categorize incoming threats and initiate predetermined reaction actions, supervised learning algorithms can be trained

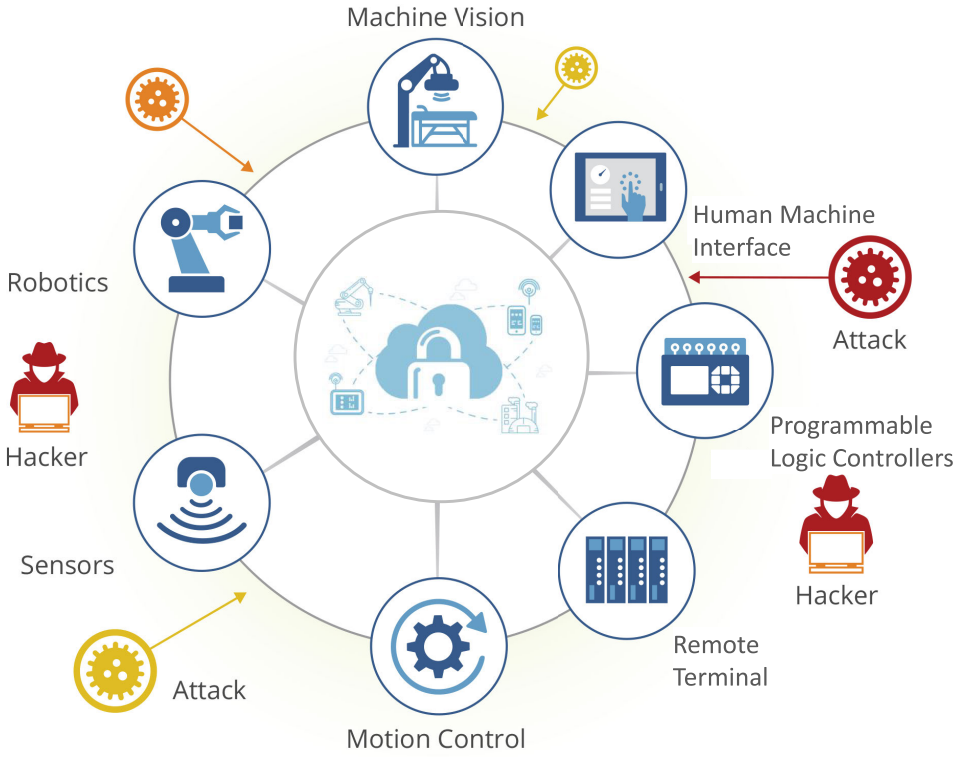

FIGURE 2. ML for cybersecurity Industry 4.0.

on labeled datasets of known cyber threats [93]. In order to prioritize and correlate security alerts, expedite incident triage, and automate response workflows, these platforms interact with security information and event management (SIEM) systems [104]. Techniques for reinforcement learning show promise for autonomous incident resolution, adaptive security policies, and dynamic threat response [105].

ML has emerged as a powerful tool for enhancing cyber resilience by automating key cybersecurity tasks and enabling adaptive defenses. However, while ML offers numerous advantages, it also presents certain limitations that organizations must consider when deploying ML-based solutions in Industry 4.0 environments. ML algorithms can automate repetitive tasks such as threat detection, incident response, and risk assessment, allowing security teams to focus on more strategic initiatives [93]. ML-based solutions can scale to analyze vast amounts of data from diverse sources, enabling organizations to monitor and protect large-scale industrial systems effectively [87]. ML models can adapt to changing cyber threats and evolving attack techniques by continuously learning from new data and adjusting their detection capabilities [106]. ML algorithms can identify subtle patterns and anomalies in data that may go unnoticed by traditional rule-based systems, improving the accuracy and efficacy of threat detection [107]. ML-based systems can respond to cyber threats in real-time, reducing the time between detection and mitigation and minimizing the impact of security incidents [108].

However, there are limitations to using ML for cyber resilience. ML algorithms require large volumes of high-quality labeled data for training, which may be scarce or difficult to obtain in cybersecurity domains [35]. ML models are susceptible to bias and unfairness, which can lead to erroneous decisions or discriminatory outcomes, particularly when trained on biased datasets [109]. ML models are vulnerable to adversarial attacks, where adversaries manipulate input data to deceive or evade detection, leading to model degradation or misclassification [110]. Many ML algorithms, such as deep neural networks, are inherently complex and lack interpretability, making it challenging to understand the rationale behind their decisions [111]. ML models may overfit to specific training data or fail to generalize to unseen data, leading to reduced performance in real-world scenarios [112].

V. ML APPLICATIONS IN CYBER RESILIENCE

A. INTRUSION DETECTION

Through the identification and remediation of harmful activity or unauthorized access within a network, intrusion detection plays a part in protecting against cyber threats. Because machine learning algorithms can sort through large amounts of data and find patterns that might point to cyberattacks, they are becoming more popular in intrusion

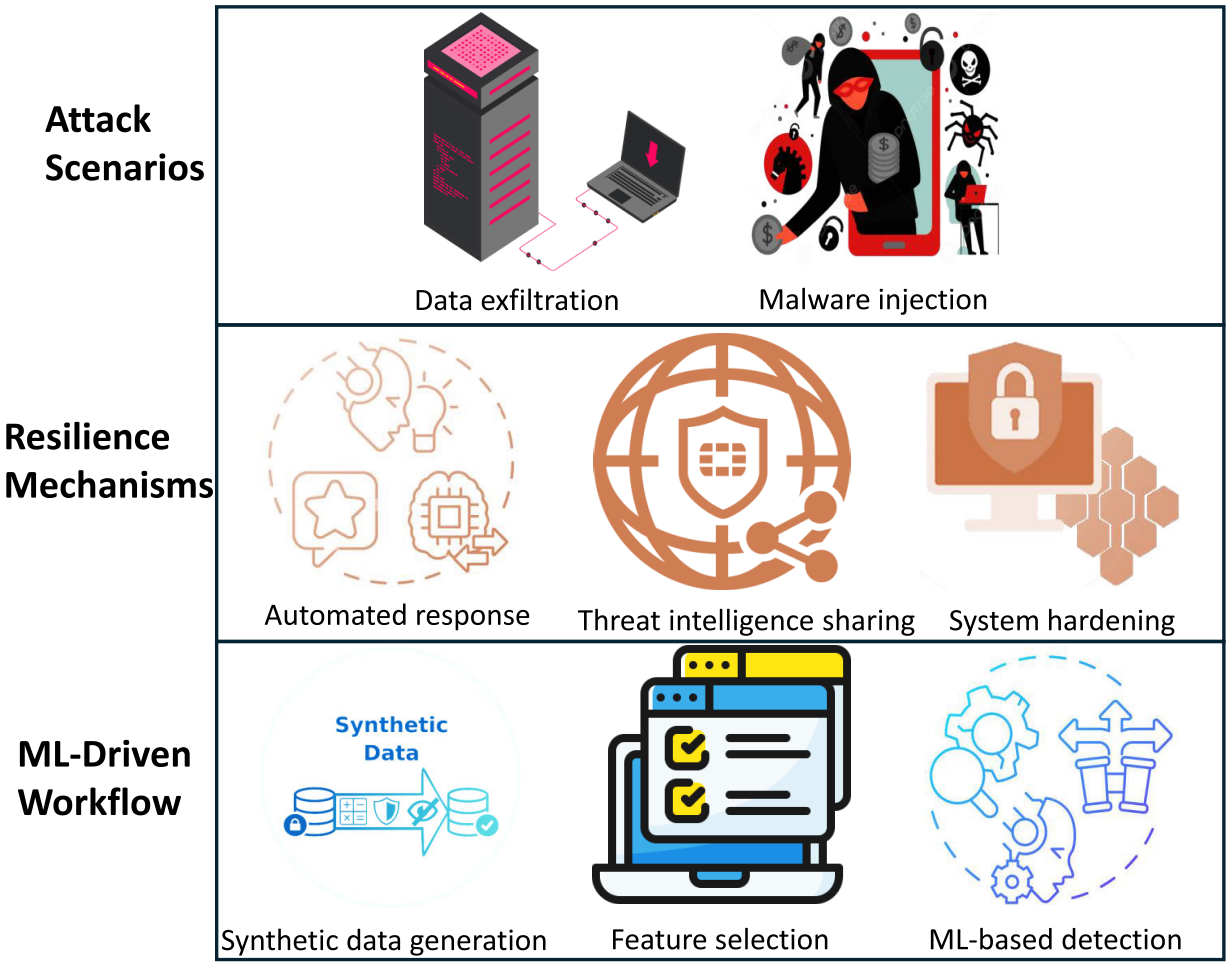

FIGURE 3. ML-driven cybersecurity resilience in industry 4.0 with mapping IIoT threats to detection and defense mechanisms.

detection. Cyber invasions can be successfully detected and stopped by using techniques used by contemporary machine learning-based intrusion detection systems. These systems scan system logs, network traffic, and other data sources for indications of malicious intent using semi-supervised learning techniques [106].

Supervised learning models, such as deep neural networks, decision trees, and support vector machines (SVMs), are trained using datasets tagged with instances of anomalous network activity [113]. They acquire the ability to distinguish between malicious activity and user behaviors by using information from packets, content payloads, and traffic patterns, among other sources. Conversely, unsupervised learning models, such as autoencoders and clustering algorithms, examine data to find anomalies or deviations that could point to hacking attempts [114]. The models can flag behaviors. Raise alerts for further investigation even without the need, for pre-labeled training data [115], [116]. Semi supervised learning methods blend. Unlabeled data to enhance the accuracy and scalability of intrusion detection [117]. These models use a set of labeled data, for training while employing learning techniques to generalize to new data and adapt to evolving security threats [118].

ML has shown promise in identifying. preventing cyber-attacks on systems by allowing for quick incident response, real-time threat detection, and flexible defenses. These algorithms examine a range of data sources, including sensor readings, system logs, and network traffic, in order to identify patterns that could point to cyberattacks [119]. By examining trends and identifying departures from typical behavior, machine learning-powered intrusion detection systems may recognize cyber threats such as malware infections, insider breaches, and advanced persistent threats (APTs) [132]. Over time, machine learning algorithms can improve detection accuracy and resilience by adapting to evolving cyber threats and gaining insights from data [106]. In order to prioritize events, link alerts, and automate response processes, machine learning-powered intrusion detection systems may easily interact with pre-existing security frameworks such as security information and event management (SIEM) systems [104]. Table.4 describes ML models and their benefits for intrusion detection.

TABLE 4. ML models for intrusion detection.

ML Model	Description	Advantages	Limitations
Decision Trees	Hierarchical tree-like structures for decision-making	Easy to interpret and visualize	Prone to overfitting
Random Forests	Ensemble learning technique	Improved generalization and robustness	Computational complexity
Support Vector Machines	Constructs hyperplanes in high-dimensional space	Effective for complex decision boundaries	Requires careful parameter tuning
Neural Networks	Models inspired by the human brain's structure	Can learn complex patterns and relationships	Require large amounts of data and resources

B. RISK ASSESSMENT

Risk assessment plays a key role in cyber resilience by helping to rank cybersecurity threats according to likelihood and possible consequences. Machine learning techniques help in this process by employing data-driven ways to efficiently identify, investigate, and resolve cyber threats. Different machine learning-based risk assessment methodologies utilize techniques to analyze incident data, contextual details, and threat intelligence, for predicting and quantifying cyber risks. These methodologies apply reinforcement learning methods to create models that can estimate the probability and severity of specific cyber threats [133].

Supervised learning models like regression random forests and gradient boosting machines are trained on labeled incident datasets to develop predictive models that assess the chances of future cyber threats occurring [134]. These models consider multiple risk factors such as vulnerabilities, threat intelligence, and organizational assets to pinpoint high-risk zones and suggest mitigation plans. On the other hand, unsupervised learning models that examine data to find hidden patterns or anomalies that point to possible new hazards include clustering algorithms and anomaly detection techniques [115]. These models detect departures from typical patterns of behavior. Even in the absence of previously labeled training data, generate warnings for potential cyber risks. Reinforcement learning models are designed to learn how to engage with an environment by making decisions that either increase rewards or decrease penalties [135]. The application of reinforcement learning techniques offers promise for controlling risks, modifying security measures, and making judgments, even if it is not frequently employed for risk assessment [136].

Machine learning works wonders in Industry 4.0 contexts, assisting companies in proactively identifying vulnerabilities, anticipating attack vectors, and allocating resources to reduce cyber threats. This helps enterprises identify and mitigate cyber threats [137]. Organizations may efficiently manage resources, prioritize security expenditures, and develop plans to address vulnerabilities and threats discovered by utilizing machine learning-based risk assessment methodologies. Utilizing analytics powered by machine learning algorithms enables enterprises to anticipate cyberattacks, modify security protocols appropriately, and react quickly to changing threat environments in real-time [74]. Machine learning-guided risk assessment frameworks may be easily integrated with current security systems, such as threat intelligence feeds and risk management platforms, to provide an overview of cyber hazards and aid in well-informed decision-making [49]. Table.5 summarizes the role of ML in risk assessment.

C. INCIDENT RESPONSE

Incident response is an element, of cyber resilience focusing on spotting examining, and minimizing the impact of cyber threats in time. Machine learning techniques provide tools for automating incident response empowering organizations to react swiftly and effectively to cyber threats. Automated incident response plans utilize machine learning algorithms to analyze security alerts link events and trigger responses instantly. These plans involve methods aimed at automating tasks streamlining incident assessment and coordinating response procedures.

Machine learning models trained on labeled datasets containing cyber threats can categorize security alerts and prioritize incidents based on their severity and potential consequences [93]. These models enable automated decision-making and response coordination reducing the time taken between detection and mitigation. Machine learning algorithms can examine telemetry data from sources like network traffic, system logs, and sensor readings to pinpoint irregularities that may signal cyber attacks [96]. Unsupervised learning methods such as clustering and autoencoders help organizations identify deviations from behavior and generate alerts for scrutiny.

Machine learning plays a role, in integrating incident response workflows by allowing organizations to automate response measures link security alerts together, and adaptively respond to evolving cyber threats. ML algorithms can examine data coming from security sensors, endpoints, and network devices to identify cyber threats, in real-time [138]. This technology empowers organizations to react promptly to security breaches and lessen their impact on business operations.

Incident response platforms powered by ML can seamlessly integrate with existing security structures like security information and event management (SIEM) systems and security automation and orchestration (SOAR) platforms. By coordinating response workflows and automating actions these platforms help organizations streamline incident assessment prioritize response efforts and optimize resource allo-

TABLE 5. ML techniques for risk assessment.

ML Technique	Description	Advantages	Limitations
Logistic Regression	Linear regression model	Simple and interpretable	Limited flexibility for complex data
Naive Bayes	Probabilistic classifier	Simple and fast	Assumes feature independence
Gradient Boosting	Ensemble learning technique	High predictive accuracy	Sensitive to noisy data
Neural Networks	Deep learning models	Learn complex patterns	Requires large datasets and computational power

cation. ML algorithms can draw insights from incident data. Adjust security measures dynamically to counter evolving cyber threats [103]. This capability allows organizations to modify security controls update access permissions and deploy measures in time for an effective response, to changing threat scenarios. ML techniques for incident response are summarized in Table.6.

D. THREAT INTELLIGENCE SHARING

To increase cyber resilience, sharing threat intelligence is essential since it enables companies to collaborate and exchange knowledge about cyber threats. Through the use of machine learning algorithms, people may share real-time threat knowledge and collaborate on defensive plans to improve situational awareness and successfully manage cyber threats. Platforms driven by machine learning for sharing real time threat intelligence use analytics and automation to gather, analyze, and distribute threat information among industry partners. These platforms enable organizations to cooperate on detecting threats responding to incidents and devising mitigation plans instantly.

Machine learning algorithms examine various data sources like network traffic, system logs, and threat feeds to spot emerging cyber threats in time [106]. These algorithms help automate threat detection for organizations and prioritize alerts based on their severity and potential impact. Machine learning-driven platforms analyze details such as attack methods, tactics, and techniques to pinpoint correlations or patterns that indicate cyber attacks [139]. By integrating threat intelligence with contextual analysis organizations can enhance their comprehension of cyber threats. Enhance their response capabilities.

Because machine learning helps firms go through large amounts of data, discover new hazards, and work together to identify and mitigate problems, it plays a function in enhancing information sharing and situational awareness among industry participants [93]. By enabling companies to communicate best practices for exchanging threat intelligence and coordinate response activities, ML-powered platforms help defense. Using ML algorithms, for instant threat analysis and decision-making helps organizations enhance their defenses and effectively reduce cyber risks. These algorithms can simulate the progression of cyber threats. Forecast their effects, on industrial systems [140]. Through examination of threat data and adjustments to threat models organizations can predict threats and take preemptive measures to manage risks proactively. Table.7 discusses the ML techniques for threat intelligence sharing highlighting the benefits.

E. SECURING ML MODELS AGAINST ADVERSARIAL ATTACKS

Adversarial attacks present a risk, to the effectiveness and dependability of machine learning models used in cybersecurity applications. It is crucial to safeguard ML models from manipulation and evasion attacks to ensure the strength and durability of cybersecurity solutions. Defending ML models against attacks necessitates the creation of defense mechanisms and strategies for dealing with such threats. Adversarial training involves augmenting the training dataset with adversarial examples generated using techniques such as the Fast Gradient Sign Method (FGSM) or Projected Gradient Descent (PGD) [141]. By exposing the model to adversarial examples during training, adversarial training aims to improve the model's robustness to such attacks. Various defense mechanisms have been proposed to detect and mitigate adversarial attacks at inference time, including input preprocessing, feature squeezing, and adversarial example detection [42]. The mechanisms aim to identify and filter out adversarial inputs before they can cause harm to the ML model. Certified robustness techniques offer assurances regarding an ML model's resilience against attacks within specific input space regions [142]. By certifying a model's robustness these approaches provide guarantees of its security and ability to withstand challenges.

The qualities of robustness and resilience are crucial for machine learning-based cybersecurity solutions, in changing and hostile environments. To maintain effective cyber defenses and reduce the likelihood of successful assaults, it is imperative to ensure the security and dependability of machine learning models. Strong machine learning models foster confidence in their capacity to identify and neutralize cyber threats [143]. Organizations may reduce the possibility of false positives or false negatives and improve the credibility of their cybersecurity solutions by protecting ML models against hostile assaults. Resilient ML models remain dependable over time even as cyber threats evolve [74]. Prioritizing robustness and resilience in ML based cybersecurity solutions helps organizations ensure their continued effectiveness, in combating emerging

TABLE 6. ML techniques for incident response.

ML Technique	Description	Advantages	Limitations
Reinforcement Learning	Learns optimal actions based on feedback	Adaptive and dynamic response	Requires exploration of action space
Clustering Algorithms	Groups similar data points together	Identifies patterns in large datasets	May require parameter tuning and preprocessing
Decision Trees	Hierarchical tree-like structures for decision-making	Easy to interpret and visualize	Prone to overfitting and sensitive to noise

TABLE 7. ML techniques for threat intelligence sharing.

ML Technique	Description	Advantages	Limitations
Natural Language Processing	Analyzes and understands human language	Extracts insights from unstructured data	Performance may vary with language complexity
Graph-based Models	Represents relationships between entities as graphs	Capture complex network structures	Scalability may be an issue with large datasets
Ensemble Methods	Combine multiple models for improved performance	Increases robustness and generalization	Requires careful selection and tuning of models

threats. Strong ML models empower organizations to adapt to changing threat landscapes. Effectively address attack strategies [106]. Incorporating defense mechanisms into ML based cybersecurity solutions allows organizations to maintain defenses that can respond to evolving threats. Table.8 summarizes the ML for adversarial attack mitigation, while ML techniques for Securing ML Models Against Adversarial Attacks are discussed in Table.9.

VI. CHALLENGES AND FUTURE TRENDS

In this section, we summarize the key findings from the review of harnessing ML for cyber resilience and identify emerging trends shaping the future of cybersecurity in Industry 4.0 environments.

A. CHALLENGES

In this section, we explore the research obstacles, in utilizing ML for cybersecurity resilience. Suggest future research directions to tackle these issues. Despite the progress made in ML-driven cybersecurity solutions, there are still research challenges that impede the achievement of cyber resilience in Industry 4.0 settings.

1) ADVERSARIAL ROBUSTNESS

Adversarial attacks remain a concern, for cybersecurity solutions based on machine learning underscoring the importance of having defense mechanisms that can withstand sophisticated attacks [42]. Developing machine learning models that can resist manipulation is a pressing research challenge, necessitating approaches for detecting, mitigating, and adapting to such attacks.

2) EXPLAINABILITY AND INTERPRETABILITY

With the increasing complexity and opacity of ML models there is a rising demand for transparent and interpretable AI techniques that offer insights into model behavior and decision-making processes [144]. Improving the transparency and interpretability of ML models is vital for establishing trust and confidence in their predictions and recommendations, in cybersecurity scenarios.

3) DATA QUALITY AND DIVERSITY

The effectiveness of machine learning models heavily relies on the quality and diversity of the training data used. Therefore collecting, labeling and preprocessing data pose challenges in cybersecurity applications [138]. It is essential to ensure access to high quality datasets that accurately capture the intricacies and variations of real world cyber threats to train adaptable machine learning models.

4) PRIVACY PRESERVATION

Creating methods to protect privacy in machine learning like federated learning and differential privacy is crucial for dealing with privacy issues and promoting data handling in cybersecurity applications [145].

5) ML CHALLENGES ADDRESSED BY GENERATIVE AI AND LARGE LANGUAGE MODELS (LLMs)

With generative AI and LLMs, industry 4.0 cybersecurity can address significant ML difficulties effectively, facilitating quicker detection, better data management, and real-time reactions [146]. However, given the increased risks they bring, enterprises will need to adopt these technologies cautiously and make sure AI is used ethically and responsibly throughout their systems.

- LLMs and generative AI can solve several meaningful ML problems, particularly in intricate industrial settings. The lack of quality data is a significant obstacle. The difficulty of getting big, labeled datasets in many businesses restricts using classic machine learning methods. Using generative AI, artificial intelligence models may be trained on synthetic data that replicates real-world events and cybersecurity incidents, among other unusual or challenging-to-collect data. This is especially helpful in domains where datasets are frequently missing or

TABLE 8. ML models for adversarial attack mitigation.

ML Model	Description	Advantages	Limitations
Adversarial Training	Augments training data with adversarial examples	Improves model robustness	Increases computational complexity
Defensive Distillation	Trains models to be resistant to adversarial attacks	Provides strong defense against attacks	May sacrifice model accuracy
Adversarial Training with Adversarial Logit Pairing	Augments training with adversarial examples and uses adversarial logits for training	Improves model robustness and generalization	Increased training time and computational cost

TABLE 9. ML techniques for securing ML models against adversarial attacks.

ML Technique	Description	Advantages	Limitations
Gradient Regularization	Adds penalties to the loss function for adversarial perturbations	Improves model robustness	May reduce model accuracy
Feature Squeezing	Reduces the input space to detect adversarial examples	Efficient and simple approach	May overlook subtle adversarial perturbations
Defensive Distillation	Trains models to be resistant to adversarial attacks	Provides strong defense against attacks	May require additional computational resources

unbalanced, such as industrial automation or cybersecurity.

- Transferring learning across domains is another significant difficulty. It is difficult for many ML models to transfer information between domains. For example, a model trained on data from one manufacturing process might not transfer effectively to another process or sector. LLMs are flexible enough to work in various areas since they may be adjusted using particular, industry-relevant data. This practical information transfer enables enterprises to use machine learning for multiple purposes, from supply chain optimization to predictive maintenance, enhancing cybersecurity tactics in networked settings.
- Because of bottlenecks and delays in data processing, classical ML models frequently struggle with generating decisions in real-time. Generative AI and LLMs can examine real-time data streams, enabling instant, automatic reactions to emerging dangers or operational inefficiencies. This is especially useful in Industry 4.0, where prompt answers to abnormalities or security threats are critical. By enabling companies to respond quickly to possible threats, these models help expedite cybersecurity decision-making and enhance overall security and resilience.

B. FUTURE TRENDS

1) ADVERSARIAL DEFENSE MECHANISMS

Create strategies to defend machine learning models, against attacks making them more resilient and secure [147]. Look into ways to detect, prevent, and adapt to threats to boost the safety and dependability of cybersecurity solutions based on machine learning.

2) EXPLAINABLE AI TECHNIQUES

Study methods that make AI systems understandable and transparent shedding light on how decisions are made by machine learning models [148]. Develop approaches for clarifying model predictions identifying weaknesses in models and building trust in cybersecurity scenarios.

3) DATA-DRIVEN APPROACHES

Utilize data-driven methods to enhance the caliber and variety of training data employed in training machine learning models [149]. Investigate strategies, for augmenting, synthesizing, and simulating data to create datasets that encompass a range of cyber threats and attack scenarios.

4) PRIVACY-PRESERVING ML SOLUTIONS

Design privacy focused machine learning solutions that allow for collaboration on data while safeguarding individual privacy rights [150]. Research federated learning, homomorphic encryption and secure party computation techniques to support private data sharing and analysis, in cybersecurity contexts.

VII. CONCLUSION

In this survey, we delved into how ML intersects with cyber resilience within the realm of Industry 4.0 and explored the ML applications that support cyber resilience including identifying intrusions evaluating risks responding to incidents sharing threat intelligence, and safeguarding ML models from attacks. Throughout our dialogue, we emphasized the role of ML in facing the evolving cybersecurity challenges brought by the interconnected industrial and the increasing use of IoT. We examined the ML-driven approaches for recognizing and mitigating cyber threats underscoring how ML improves awareness automates response measures and promotes collaboration among players. Despite progress in ML based cybersecurity solutions, there are still unresolved research hurdles to overcome including adversarial resistance, interpretability concerns, data quality issues, and privacy protection. Tackling these obstacles and charting out research avenues are vital, for propelling the field of ML-powered cybersecurity and attaining robust and resilient

cyber resilience within Industry 4.0 landscapes. we explored various aspects of ML applications in enhancing cyber resilience, including intrusion detection, risk assessment, incident response, threat intelligence sharing, and securing ML models against adversarial attacks.

REFERENCES

[1] M. Javaid, A. Haleem, R. P. Singh, and R. Suman, "An integrated outlook of cyber–physical systems for Industry 4.0: Topical practices, architecture, and applications," *Green Technol. Sustainability*, vol. 1, no. 1, Jan. 2023, Art. no. 100001.

[2] S. H. Alsamhi, A. Hawbani, S. Kumar, L. Porwol, and E. Curry, "Decentralized metaverse: Towards a secure, autonomous, and inclusive virtual world," in *Proc. Int. Conf. Electr., Comput. Energy Technol. (ICECET)*, vol. 2, Nov. 2023, pp. 1–7.

[3] T. Borangiu, O. Morariu, S. Rileanu, D. Trentesaux, P. Leito, and J. Barata, "Digital transformation of manufacturing. Industry of the future with cyber-physical production systems," *Romanian J. Inf. Sci. Technol.*, vol. 23, no. 1, pp. 3–37, 2020.

[4] F. Syed, S. K. Gupta, S. H. Alsamhi, M. Rashid, and X. Liu, "A survey on recent optimal techniques for securing unmanned aerial vehicles applications," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 7, p. e4133, Jul. 2021.

[5] G. Lampropoulos and K. Siakas, "Enhancing and securing cyber-physical systems and Industry 4.0 through digital twins: A critical review," *J. Softw., Evol. Process*, vol. 35, no. 7, p. e2494, Jul. 2023.

[6] R. Tallat, A. Hawbani, X. Wang, A. Al-Dubai, L. Zhao, Z. Liu, G. Min, A. Y. Zomaya, and S. H. Alsamhi, "Navigating Industry 5.0: A survey of key enabling technologies, trends, challenges, and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 2, pp. 1080–1126, 2nd Quart., 2024.

[7] S. H. Alsamhi, A. A. F. Saif, E. Curry, S. Kumar, and A. Hawbani, "Autonomous multi-robot collaboration in virtual environments to perform tasks in Industry 4.0," in *Proc. 2nd Int. Conf. Emerg. Smart Technol. Appl. (eSmarTA)*, Oct. 2022, pp. 1–7.

[8] R. Sahal, S. H. Alsamhi, and K. N. Brown, "Digital twins collaboration in industrial manufacturing," in *Digital Twins: Basics and Applications*. Cham, Switzerland: Springer, 2022, pp. 59–72.

[9] S. H. Alsamhi, A. V. Shvetsov, A. Hawbani, S. V. Shvetsova, S. Kumar, and L. Zhao, "Survey on federated learning enabling indoor navigation for Industry 4.0 in B5G," *Future Gener. Comput. Syst.*, vol. 148, pp. 250–265, Nov. 2023.

[10] S. H. Alsamhi, A. V. Shvetsov, S. Kumar, J. Hassan, M. A. Alhartomi, S. V. Shvetsova, R. Sahal, and A. Hawbani, "Computing in the sky: A survey on intelligent ubiquitous computing for UAV-assisted 6G networks and Industry 4.0/5.0," *Drones*, vol. 6, no. 7, p. 177, Jul. 2022.

[11] S. H. Alsamhi, A. Hawbani, R. Sahal, S. Srivastava, S. Kumar, L. Zhao, M. A. A. Al-Qaness, J. Hassan, M. Guizani, and E. Curry, "Towards sustainable Industry 4.0: A survey on greening IoE in 6G networks," *Ad Hoc Netw.*, vol. 165, Dec. 2024, Art. no. 103610.

[12] S. H. Alsamhi, A. Hawbani, S. Kumar, M. Timilsina, M. Al-Qatf, R. Haque, F. M. A. Nashwan, L. Zhao, and E. Curry, "Empowering Dataspace 4.0: Unveiling promise of decentralized data-sharing," *IEEE Access*, vol. 12, pp. 112637–112658, 2024.

[13] S. H. Alsamhi, F. A. Almalki, O. Ma, M. S. Ansari, and B. Lee, "Predictive estimation of optimal signal strength from drones over IoT frameworks in smart cities," *IEEE Trans. Mobile Comput.*, vol. 22, no. 1, pp. 402–416, Jan. 2023.

[14] R. Sahal, S. H. Alsamhi, J. G. Breslin, K. N. Brown, and M. I. Ali, "Digital twins collaboration for automatic erratic operational data detection in Industry 4.0," *Appl. Sci.*, vol. 11, no. 7, p. 3186, Apr. 2021.

[15] S. H. Alsamhi, F. A. Almalki, H. Al-Dois, S. B. Othman, J. Hassan, A. Hawbani, R. Sahal, B. Lee, and H. Saleh, "Machine learning for smart environments in B5G networks: Connectivity and QoS," *Comput. Intell. Neurosci.*, vol. 2021, no. 1, Jan. 2021, Art. no. 6805151.

[16] R. Sahal, S. H. Alsamhi, and K. N. Brown, "Personal digital twin: A close look into the present and a step towards the future of personalised healthcare industry," *Sensors*, vol. 22, no. 15, p. 5918, Aug. 2022.

[17] S. H. Alsamhi, O. Ma, and M. S. Ansari, "Convergence of machine learning and robotics communication in collaborative assembly: Mobility, connectivity and future perspectives," *J. Intell. Robotic Syst.*, vol. 98, nos. 3–4, pp. 541–566, Jun. 2020.

[18] A. Saif, K. Dimyati, K. A. Noordin, S. H. Alsamhi, and A. Hawbani, "Multi-UAV and SAR collaboration model for disaster management in B5G networks," *Internet Technol. Lett.*, vol. 7, no. 1, p. e310, Jan. 2024.

[19] T. Sobb, B. Turnbull, and N. Moustafa, "Supply chain 4.0: A survey of cyber security challenges, solutions and future directions," *Electronics*, vol. 9, no. 11, p. 1864, Nov. 2020.

[20] A. Rahiminejad, J. Plotnek, R. Atallah, M.-A. Dubois, D. Malatrait, M. Ghafouri, A. Mohammadi, and M. Debbabi, "A resilience-based recovery scheme for smart grid restoration following cyberattacks to substations," *Int. J. Electr. Power Energy Syst.*, vol. 145, Feb. 2023, Art. no. 108610.

[21] F. Syed, S. H. Alsamhi, S. K. Gupta, and A. Saif, "LSB-XOR technique for securing captured images from disaster by UAVs in B5G networks," *Concurrency Comput., Pract. Exper.*, vol. 36, no. 12, p. e8061, May 2024.

[22] G. Ahmadi-Assalemi, "Anomalous behaviour detection for cyber defence in modern industrial control systems," Ph.D. thesis, School Eng., Comput. Math. Sci., Faculty Sci. Eng., Univ. Wolverhampton, 2022.

[23] F. A. Almalki, S. H. Alsamhi, and M. C. Angelides, "Internet of X-enabled intelligent unmanned aerial vehicles security for hyper-connected societies," in *Security and Privacy in Cyberspace*. Singapore: Springer, 2022, pp. 75–100.

[24] 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," *Ind. Manuf. Eng.*, 2023, doi: 10.20944/preprints202305.0529.v1.

[25] A. Cartwright and E. Cartwright, "The economics of ransomware attacks on integrated supply chain networks," *Digit. Threats, Res. Pract.*, vol. 4, no. 4, pp. 1–14, Dec. 2023.

[26] C. Hankin and M. Barrre, "Trustworthy inter-connected cyber-physical systems," in *Proc. Int. Conf. Crit. Inf. Infrastruct. Secur.* Cham, Switzerland: Springer, 2020, pp. 3–13.

[27] S. H. Alsamhi, A. V. Shvetsov, S. V. Shvetsova, A. Hawbani, M. Guizani, M. A. Alhartomi, and O. Ma, "Blockchain-empowered security and energy efficiency of drone swarm consensus for environment exploration," *IEEE Trans. Green Commun. Netw.*, vol. 7, no. 1, pp. 328–338, Mar. 2023.

[28] M. D. Cavelty and A. Wenger, "Cyber security meets security politics: Complex technology, fragmented politics, and networked science," *Contemp. Secur. Policy*, vol. 41, no. 1, pp. 5–32, Jan. 2020.

[29] A. S. George, T. Baskar, and P. B. Srikaanth, "Cyber threats to critical infrastructure: Assessing vulnerabilities across key sectors," *Partners Universal Int. Innov. J.*, vol. 2, no. 1, pp. 51–75, 2024.

[30] A. J. G. de Azambuja, C. Plesker, K. Schützer, R. Anderl, B. Schleich, and V. R. Almeida, "Artificial intelligence-based cyber security in the context of Industry 4.0—A survey," *Electronics*, vol. 12, no. 8, p. 1920, Apr. 2023.

[31] M. S. Ansari, S. H. Alsamhi, Y. Qiao, Y. Ye, and B. Lee, "Security of distributed intelligence in edge computing: Threats and countermeasures," in *The Cloud-to-Thing Continuum: Opportunities and Challenges in Cloud, Fog and Edge Computing*. Springer, 2020, pp. 95–122, doi: 10.1007/978-3-030-41110-7_6.

[32] V. O. Nyangaresi and S. H. Alsamhi, "Towards secure traffic signaling in smart grids," in *Proc. 3rd Global Power, Energy Commun. Conf. (GPECOM)*, Oct. 2021, pp. 196–201.

[33] E. Sabev, R. Trifonov, G. Pavlova, and K. Raynova, "Analysis of practical machine learning scenarios for cybersecurity in Industry 4.0," *WSEAS Trans. Syst. Control*, vol. 18, pp. 444–459, Dec. 2023.

[34] M. Abdulhussein, "The impact of artificial intelligence and ML on organizations cybersecurity," School Business, Liberty Univ., Tech. Rep., Feb. 2024. [Online]. Available: https://digitalcommons.liberty.edu/doctoral/5242/

[35] G. Apruzzese, P. Laskov, E. M. de Oca, W. Mallouli, L. B. Rapa, A. V. Grammatopoulos, and F. Di Franco, "The role of ML in cybersecurity," *Digit. Threats, Res. Pract.*, vol. 4, no. 1, pp. 1–38, 2023.

[36] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, "Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset," *IEEE Access*, vol. 9, pp. 22351–22370, 2021.

[37] S. A. Vaddadi, R. Vallabhaneni, and P. Whig, "Utilizing AI and ML in cybersecurity for sustainable development through enhanced threat detection and mitigation," *Int. J. Sustain. Develop. Through AI, ML IoT*, vol. 2, no. 2, pp. 1–8, 2023.

[38] A. Sharma, H. Sajjad, Roshani, and M. H. Rahaman, "A systematic review for assessing the impact of climate change on landslides: Research gaps and directions for future research," *Spatial Inf. Res.*, vol. 32, no. 2, pp. 165–185, Apr. 2024.

[39] A. Manoharan and M. Sarker, "Revolutionizing cybersecurity: Unleashing the power of artificial intelligence and ML for next-generation threat detection," Tech. Rep., 2023, doi: 10.56726/IRJMETS32644.
[40] A. Gupta, R. Gupta, and G. Kukreja, "Cyber security using ML : Techniques and business applications," *Appl. Artif. Intell. Bus., Educ. Healthcare*, pp. 385–406, Jul. 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:238044917
[41] P. V. Mohan, S. Dixit, A. Gyaneshwar, U. Chadha, K. Srinivasan, and J. T. Seo, "Leveraging computational intelligence techniques for defensive deception: A review, recent advances, open problems and future directions," *Sensors*, vol. 22, no. 6, p. 2194, Mar. 2022.
[42] M. Khan and L. Ghafoor, "Adversarial ML in the context of network security: Challenges and solutions," *J. Comput. Intell. Robot.*, vol. 4, no. 1, pp. 51–63, 2024.
[43] A. Alotaibi and M. A. Rassam, "Adversarial machine learning attacks against intrusion detection systems: A survey on strategies and defense," *Future Internet*, vol. 15, no. 2, p. 62, Jan. 2023.
[44] W. A. Ali, K. N. Manasa, M. Bendechache, M. F. Aljunaid, and P. Sandhya, "A review of current machine learning approaches for anomaly detection in network traffic," *J. Telecommun. Digit. Economy*, vol. 8, no. 4, pp. 64–95, 2020.
[45] T. Tagarev and G. Sharkov, "Computationally intensive functions in designing and operating distributed cyber secure and resilient systems," in *Proc. 20th Int. Conf. Comput. Syst. Technol.*, vol. 68, Jun. 2019, pp. 8–18.
[46] D. A. S. Estay, R. Sahay, M. B. Barfod, and C. D. Jensen, "A systematic review of cyber-resilience assessment frameworks," *Comput. Secur.*, vol. 97, Oct. 2020, Art. no. 101996.
[47] S. F. Mihalache, E. Pricop, and J. Fattahi, "Resilience enhancement of cyber-physical systems: A review," in *Power Systems Resilience: Modeling, Analysis and Practice*. Springer, 2019, pp. 269–287, doi: 10.1007/978-3-319-94442-5_11.
[48] Y. Kannan, "Federated learning in cybersecurity: Applications, challenges, and future directions," *Int. J. Sci. Res.*, vol. 13, no. 7, pp. 617–622, Jul. 2024.
[49] U. I. Okoli, O. C. Obi, A. O. Adewusi, and T. O. Abrahams, "Machine learning in cybersecurity: A review of threat detection and defense mechanisms," *World J. Adv. Res. Rev.*, vol. 21, no. 1, pp. 2286–2295, Jan. 2024.
[50] E. Anthi, L. Williams, M. Rhode, P. Burnap, and A. Wedgbury, "Adversarial attacks on machine learning cybersecurity defences in industrial control systems," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102717.
[51] J. Uzoma, O. Falana, C. Obunadike, K. Oloyede, and E. Obunadike, "Using artificial intelligence for automated incidence response in cyber-security," *Int. J. Inf. Technol.*, vol. 1, no. 4, pp. 1–32, 2023.
[52] P. Mahadevappa, R. K. Murugesan, R. Al-Amri, R. Thabit, A. H. Al-Ghushami, and G. Alkawsi, "A secure edge computing model using machine learning and IDS to detect and isolate intruders," *MethodsX*, vol. 12, Jun. 2024, Art. no. 102597.
[53] V. Thapliyal and P. Thapliyal, "Machine learning for cybersecurity: Threat detection, prevention, and response," *Darpan Int. Res. Anal.*, vol. 12, no. 1, pp. 1–7, Feb. 2024.
[54] B. Kumar, "Cyber threat intelligence using AI and machine learning approaches," *Int. J. Bus. Manag. Visuals*, vol. 6, no. 1, pp. 43–49, 2023.
[55] M. Mijwil, I. E. Salem, and M. M. Ismaeel, "The significance of machine learning and deep learning techniques in cybersecurity: A comprehensive review," *Iraqi J. Comput. Sci. Math.*, vol. 4, no. 1, pp. 87–101, 2023.
[56] J. P. Bharadiya, "AI-driven security: How machine learning will shape the future of cybersecurity and web 3.0," *Amer. J. Neural Netw. Appl.*, vol. 9, no. 1, pp. 1–7, 2023.
[57] A. Deshmukh, D. S. Patil, G. Soni, and A. K. Tyagi, "Cyber security: New realities for Industry 4.0 and Society 5.0," in *Handbook of Research on Quantum Computing for Smart Environments*. Hershey, PA, USA: IGI Global, 2023, pp. 299–325.
[58] A. N. Kia, F. Murphy, B. Sheehan, and D. Shannon, "A cyber risk prediction model using common vulnerabilities and exposures," *Expert Syst. Appl.*, vol. 237, Mar. 2024, Art. no. 121599.
[59] C.-A. Brust, "Semantic knowledge integration for learning from semantically imprecise data," Ph.D. thesis, Friedrich-Schiller-Universität Jena Fakultät für Mathematik und Informatik Lehrstuhl für Digitale Bildverarbeitung, 2022. [Online]. Available: https://www.db-thueringen.de/receive/dbt_mods_00051899
[60] J. C. N. Bittencourt, D. G. Costa, P. Portugal, and F. Vasques, "A data-driven clustering approach for assessing spatiotemporal vulnerability to urban emergencies," *Sustain. Cities Soc.*, vol. 108, Aug. 2024, Art. no. 105477.
[61] M. Asmar and A. Tuqan, "Integrating machine learning for sustaining cybersecurity in digital banks," *Heliyon*, vol. 10, no. 17, Sep. 2024, Art. no. e37571.
[62] S. B. Chafjiri, P. Legg, J. Hong, and M.-A. Tsompanas, "Vulnerability detection through machine learning-based fuzzing: A systematic review," *Comput. Secur.*, vol. 143, Aug. 2024, Art. no. 103903.
[63] Z. Huang, X. Yu, D. Zhu, and M. C. Hughes, "InterLUDE: Interactions between labeled and unlabeled data to enhance semi-supervised learning," 2024, *arXiv:2403.10658*.
[64] M. Amouei, M. Rezvani, and M. Fateh, "RAT: Reinforcement-learning-driven and adaptive testing for vulnerability discovery in web application firewalls," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 5, pp. 3371–3386, Sep. 2022.
[65] Z. Wang and T. Hong, "Reinforcement learning for building controls: The opportunities and challenges," *Appl. Energy*, vol. 269, Jul. 2020, Art. no. 115036.
[66] M. A. Ibrahim and S. Askar, "An intelligent scheduling strategy in fog computing system based on multi-objective deep reinforcement learning algorithm," *IEEE Access*, vol. 11, pp. 133607–133622, 2023.
[67] S. E. Hamdi, A. Abouabdellah, and M. Oudani, "Industry 4.0: Fundamentals and main challenges," in *Proc. Int. Colloq. Logistics Supply Chain Manag. (LOGISTIQUA)*, Jun. 2019, pp. 1–5.
[68] L. B. Furstenau, M. K. Sott, L. M. Kipper, E. L. Machado, J. R. Lopez-Robles, M. S. Dohan, M. J. Cobo, A. Zahid, Q. H. Abbasi, and M. A. Imran, "Link between sustainability and Industry 4.0: Trends, challenges and new perspectives," *IEEE Access*, vol. 8, pp. 140079–140096, 2020.
[69] E. Fazeldehkordi and T.-M. Grønli, "A survey of security architectures for edge computing-based IoT," *IoT*, vol. 3, no. 3, pp. 332–365, Jun. 2022.
[70] W. Hu and Y. Tan, "Generating adversarial malware examples for black-box attacks based on GAN," in *Proc. Int. Conf. Data Mining Big Data*. Singapore: Springer, 2022, pp. 409–423.
[71] G. Apruzzese, M. Colajanni, and M. Marchetti, "Evaluating the effectiveness of adversarial attacks against botnet detectors," in *Proc. IEEE 18th Int. Symp. Netw. Comput. Appl. (NCA)*, Sep. 2019, pp. 1–8.
[72] S. H. Alsamhi, S. Kumar, A. Hawbani, A. V. Shvetsov, L. Zhao, and M. Guizani, "Synergy of human-centered AI and cyber-physical-social systems for enhanced cognitive situation awareness: Applications, challenges and opportunities," *Cogn. Comput.*, vol. 16, no. 5, pp. 2735–2755, Sep. 2024.
[73] M. F. Arroyabe, C. F. A. Arranz, I. F. de Arroyabe, and J. C. F. de Arroyabe, "The effect of IT security issues on the implementation of Industry 4.0 in SMEs: Barriers and challenges," *Technolog. Forecasting Social Change*, vol. 199, Feb. 2024, Art. no. 123051.
[74] M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking cyber threats: A framework for the future of cybersecurity," *Sustainability*, vol. 15, no. 18, p. 13369, Sep. 2023.
[75] B. I. Mukhtar, M. S. Elsayed, A. D. Jurcut, and M. A. Azer, "IoT vulnerabilities and attacks: SILEX malware case study," *Symmetry*, vol. 15, no. 11, p. 1978, Oct. 2023.
[76] J.-P.-A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," *Microprocessors Microsyst.*, vol. 77, Sep. 2020, Art. no. 103201.
[77] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments," *Energy Rep.*, vol. 7, pp. 8176–8186, Nov. 2021.
[78] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review," *Sensors*, vol. 23, no. 8, p. 4117, Apr. 2023.
[79] A. G. Silva-Trujillo, M. J. G. González, L. P. Rocha Pérez, and L. J. G. Villalba, "Cybersecurity analysis of wearable devices: Smartwatches passive attack," *Sensors*, vol. 23, no. 12, p. 5438, Jun. 2023.
[80] M. Liyanage, A. Braeken, S. Shahabuddin, and P. Ranaweera, "Open RAN security: Challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 214, May 2023, Art. no. 103621.
[81] F. Mokbal, W. Dan, M. Osman, Y. Ping, and S. Alsamhi, "An efficient intrusion detection framework based on embedding feature selection and ensemble learning technique," *Int. Arab J. Inf. Technol.*, vol. 19, no. 2, pp. 237–248, 2022.
[82] M. Hijji and G. Alam, "Cybersecurity awareness and training (CAT) framework for remote working employees," *Sensors*, vol. 22, no. 22, p. 8663, Nov. 2022.
[83] B. Dupont, C. Shearing, M. Bernier, and R. Leukfeldt, "The tensions of cyber-resilience: From sensemaking to practice," *Comput. Secur.*, vol. 132, Sep. 2023, Art. no. 103372.

[84] S. Chen, Z. Wu, and P. D. Christofides, "Cyber-attack detection and resilient operation of nonlinear processes under economic model predictive control," *Comput. Chem. Eng.*, vol. 136, May 2020, Art. no. 106806.
[85] S. Duchek, S. Raetze, and I. Scheuch, "The role of diversity in organizational resilience: A theoretical framework," *Bus. Res.*, vol. 13, no. 2, pp. 387–423, Jul. 2020.
[86] I. Arshad, S. H. Alsamhi, Y. Qiao, B. Lee, and Y. Ye, "IOTM: Iterative optimization trigger method—A runtime data-free backdoor attacks on deep neural networks," *IEEE Trans. Artif. Intell.*, vol. 5, no. 9, pp. 4562–4573, Sep. 2024.
[87] I. H. Sarker, "Machine learning: Algorithms, real-world applications and research directions," *Social Netw. Comput. Sci.*, vol. 2, no. 3, p. 160, May 2021.
[88] Q. Wang, Y. Ma, K. Zhao, and Y. Tian, "A comprehensive survey of loss functions in machine learning," *Ann. Data Sci.*, vol. 9, no. 2, pp. 187–212, Apr. 2022.
[89] Z. Khandezamin, M. Naderan, and M. J. Rashti, "Detection and classification of breast cancer using logistic regression feature selection and GMDH classifier," *J. Biomed. Informat.*, vol. 111, Nov. 2020, Art. no. 103591.
[90] J. Lee, J. Kim, I. Kim, and K. Han, "Cyber threat detection based on artificial neural networks using event profiles," *IEEE Access*, vol. 7, pp. 165607–165626, 2019.
[91] P. Zhang, W. Ma, and S. Qian, "Cluster analysis of day-to-day traffic data in networks," *Transp. Res. C, Emerg. Technol.*, vol. 144, Nov. 2022, Art. no. 103882.
[92] B. G. Sarmina, G.-H. Sun, and S.-H. Dong, "Principal component analysis and t-distributed stochastic neighbor embedding analysis in the study of quantum approximate optimization algorithm entangled and non-entangled mixing operators," *Entropy*, vol. 25, no. 11, p. 1499, Oct. 2023.
[93] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Inf. Fusion*, vol. 97, Sep. 2023, Art. no. 101804.
[94] C.-Y. Hsu, S. Wang, and Y. Qiao, "Intrusion detection by machine learning for multimedia platform," *Multimedia Tools Appl.*, vol. 80, no. 19, pp. 29643–29656, Aug. 2021.
[95] Z. Dang, Y. Zheng, X. Lin, C. Peng, Q. Chen, and X. Gao, "Semi-supervised learning for anomaly traffic detection via bidirectional normalizing flows," 2024, *arXiv:2403.10550*.
[96] F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, "Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models," *Internet Things Cyber-Phys. Syst.*, vol. 4, pp. 167–185, Jan. 2024.
[97] A. Chatterjee and B. S. Ahmed, "IoT anomaly detection methods and applications: A survey," *Internet Things*, vol. 19, Aug. 2022, Art. no. 100568.
[98] P. Cheimonidis and K. Rantos, "Dynamic risk assessment in cybersecurity: A systematic literature review," *Future Internet*, vol. 15, no. 10, p. 324, Sep. 2023.
[99] I. H. Sarker, "Machine learning for intelligent data analysis and automation in cybersecurity: Current and future prospects," *Ann. Data Sci.*, vol. 10, no. 6, pp. 1473–1498, Dec. 2023.
[100] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience," *Sensors*, vol. 23, no. 16, p. 7273, Aug. 2023.
[101] M. Dolores, C. Fernandez-Basso, J. Gómez-Romero, and M. J. Martin-Bautista, "A big data association rule mining based approach for energy building behaviour analysis in an IoT environment," *Sci. Rep.*, vol. 13, no. 1, p. 19810, Nov. 2023.
[102] S. Kalogiannidis, D. Kalfas, O. Papaevangelou, G. Giannarakis, and F. Chatzitheodoridis, "The role of artificial intelligence technology in predictive risk assessment for business Continuity: A case study of Greece," *Risks*, vol. 12, no. 2, p. 19, Jan. 2024.
[103] M. Ahsan, K. E. Nygard, R. Gomes, M. M. Chowdhury, N. Rifat, and J. F. Connolly, "Cybersecurity threats and their mitigation approaches using machine learning—A review," *J. Cybersecur. Privacy*, vol. 2, no. 3, pp. 527–555, Jul. 2022.
[104] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures," *Sensors*, vol. 21, no. 14, p. 4759, Jul. 2021.
[105] S. H. Oh, J. Kim, J. H. Nah, and J. Park, "Employing deep reinforcement learning to cyber-attack simulation for enhancing cybersecurity," *Electronics*, vol. 13, no. 3, p. 555, Jan. 2024.
[106] N. Mohamed, "Current trends in AI and ML for cybersecurity: A state-of-the-art survey," *Cogent Eng.*, vol. 10, no. 2, Dec. 2023, Art. no. 2272358.
[107] M. M. Inuwa and R. Das, "A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks," *Internet Things*, vol. 26, Jul. 2024, Art. no. 101162.
[108] S. A. Vaddadi, R. Vallabhaneni, and P. Whig, "Utilizing AI and machine learning in cybersecurity for sustainable development through enhanced threat detection and mitigation," *Int. J. Sustain. Develop. Through AI, ML IoT*, vol. 2, no. 2, pp. 1–8, 2023.
[109] T. D. Jui and P. Rivas, "Fairness issues, current approaches, and challenges in machine learning models," *Int. J. Mach. Learn. Cybern.*, vol. 15, no. 8, pp. 3095–3125, Aug. 2024.
[110] M. Macas, C. Wu, and W. Fuertes, "Adversarial examples: A survey of attacks and defenses in deep learning-enabled cybersecurity systems," *Expert Syst. Appl.*, vol. 238, Mar. 2024, Art. no. 122223.
[111] P. Linardatos, V. Papastefanopoulos, and S. Kotsiantis, "Explainable AI: A review of machine learning interpretability methods," *Entropy*, vol. 23, no. 1, p. 18, Dec. 2020.
[112] C. Aliferis and G. Simon, "Overfitting, underfitting and general model overconfidence and under-performance pitfalls and best practices in machine learning and AI," in *Artificial Intelligence and Machine Learning in Health Care and Medical Sciences: Best Practices and Pitfalls*. Cham, Switzerland: Springer, 2024, pp. 477–524.
[113] S. H. Rafique, A. Abdallah, N. S. Musa, and T. Murugan, "Machine learning and deep learning techniques for Internet of Things network anomaly detection—Current research trends," *Sensors*, vol. 24, no. 6, p. 1968, Mar. 2024.
[114] P. Dini, A. Elhanashi, A. Begni, S. Saponara, Q. Zheng, and K. Gasmi, "Overview on intrusion detection systems design exploiting machine learning for networking cybersecurity," *Appl. Sci.*, vol. 13, no. 13, p. 7507, Jun. 2023.
[115] W.-H. Choi and J. Kim, "Unsupervised learning approach for anomaly detection in industrial control systems," *Appl. Syst. Innov.*, vol. 7, no. 2, p. 18, Feb. 2024.
[116] M. Landauer, S. Onder, F. Skopik, and M. Wurzenberger, "Deep learning for anomaly detection in log data: A survey," *Mach. Learn. Appl.*, vol. 12, Jun. 2023, Art. no. 100470.
[117] R.-H. Hwang, T.-H. Tsai, and J.-Y. Lin, "Intrusion detection system using semi-supervised learning with hybrid labeling techniques," in *Proc. Int. Conf. Adv. Inf. Commun. Technol.* Cham, Switzerland: Springer, 2023, pp. 77–85.
[118] J. Wang and F. Biljecki, "Unsupervised machine learning in urban studies: A systematic review of applications," *Cities*, vol. 129, Oct. 2022, Art. no. 103925.
[119] A. M. Y. Koay, R. K. L. Ko, H. Hettema, and K. Radke, "Machine learning in industrial control system (ICS) security: Current landscape, opportunities and challenges," *J. Intell. Inf. Syst.*, vol. 60, no. 2, pp. 377–405, Apr. 2023.
[120] M. Saqib and A. H. Moon, "A systematic security assessment and review of Internet of Things in the context of authentication," *Comput. Secur.*, vol. 125, Feb. 2023, Art. no. 103053.
[121] V. Hassija, V. Chamola, V. Gupta, S. Jain, and N. Guizani, "A survey on supply chain security: Application areas, security threats, and solution architectures," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6222–6246, Apr. 2021.
[122] D. D. Sam and X. Liu, "The impact of system outages on national critical infrastructure sectors: Cybersecurity practitioners' perspective," *Issues Inf. Syst.*, vol. 24, no. 4, 2023, doi: 10.48009/4_iis_2023_121.
[123] S. H. Alsamhi, R. Myrzashova, A. Hawbani, S. Kumar, S. Srivastava, L. Zhao, X. Wei, M. Guizan, and E. Curry, "Federated learning meets blockchain in decentralized data sharing: Healthcare use case," *IEEE Internet Things J.*, vol. 11, no. 11, pp. 19602–19615, Jun. 2024.
[124] T. Kim, J. Ochoa, T. Faika, H. A. Mantooth, J. Di, Q. Li, and Y. Lee, "An overview of cyber-physical security of battery management systems and adoption of blockchain technology," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 10, no. 1, pp. 1270–1281, Feb. 2022.
[125] R. Myrzashova, S. H. Alsamhi, A. Hawbani, E. Curry, M. Guizani, and X. Wei, "Safeguarding patient data-sharing: Blockchain-enabled federated learning in medical diagnostics," *IEEE Trans. Sustain. Comput.*, early access, Jun. 4, 2024, doi: 10.1109/TSUSC.2024.3409329.

[126] T. Sasi, A. H. Lashkari, R. Lu, P. Xiong, and S. Iqbal, "A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges," *J. Inf. Intell.*, vol. 2, no. 6, pp. 455–513, Nov. 2024.
[127] A. C. Panchal, V. M. Khadse, and P. N. Mahalle, "Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures," in *Proc. IEEE Global Conf. Wireless Comput. Netw. (GCWCN)*, Nov. 2018, pp. 124–130.
[128] H.-M. Kim and K.-H. Lee, "IIoT malware detection using edge computing and deep learning for cybersecurity in smart factories," *Appl. Sci.*, vol. 12, no. 15, p. 7679, Jul. 2022.
[129] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Secur. Appl.*, vol. 2, Jan. 2024, Art. no. 100031.
[130] G. Czeczot, I. Rojek, D. Mikołajewski, and B. Sangho, "AI in IIoT management of cybersecurity for Industry 4.0 and Industry 5.0 purposes," *Electronics*, vol. 12, no. 18, p. 3800, Sep. 2023.
[131] M. Ni, "A review on machine learning methods for intrusion detection system," *Appl. Comput. Eng.*, vol. 27, no. 1, pp. 57–64, Dec. 2023.
[132] D. T. Salim, M. M. Singh, and P. Keikhosrokiani, "A systematic literature review for APT detection and effective cyber situational awareness (ECSA) conceptual model," *Heliyon*, vol. 9, no. 7, Jul. 2023, Art. no. e17156.
[133] C. Bellas, A. Naskos, G. Kougka, G. Vlahavas, A. Gounaris, A. Vakali, A. Papadopoulos, E. Biliri, N. Bountouni, and G. G. Granadillo, "A methodology for runtime detection and extraction of threat patterns," *Social Netw. Comput. Sci.*, vol. 1, no. 5, pp. 1–13, Sep. 2020.
[134] J. K. Afriyie, K. Tawiah, W. A. Pels, S. Addai-Henne, H. A. Dwamena, E. O. Owiredu, S. A. Ayeh, and J. Eshun, "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions," *Decis. Anal. J.*, vol. 6, Mar. 2023, Art. no. 100163.
[135] M. Ghasemi, A. H. Moosavi, I. Sorkhoh, A. Agrawal, F. Alzhouri, and D. Ebrahimi, "An introduction to reinforcement learning: Fundamental concepts and practical applications," 2024, *arXiv:2408.07712*.
[136] P. V. Rao, B. Vybhavi, M. Manjeet, A. Kumar, M. Mittal, A. Verma, and D. Dhabliya, "Deep reinforcement learning: Bridging the gap with neural networks," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 15s, pp. 576–586, 2024.
[137] A. T. Oyewole, C. C. Okoye, O. C. Ofodile, and C. E. Ugochukwu, "Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio," *World J. Adv. Res. Rev.*, vol. 21, no. 3, pp. 625–643, Mar. 2024.
[138] N. G. Camacho, "The role of AI in cybersecurity: Addressing threats in the digital age," *J. Artif. Intell. Gen. Sci.*, vol. 3, no. 1, pp. 143–154, Mar. 2024.
[139] E. Ortiz-Ruiz, J. R. Bermejo, J. A. Sicilia, and J. Bermejo, "Machine learning techniques for cyberattack prevention in IoT systems: A comparative perspective of cybersecurity and cyberdefense in Colombia," *Electronics*, vol. 13, no. 5, p. 824, Feb. 2024.
[140] O. A. Ajala, C. C. Okoye, O. C. Ofodile, C. A. Arinze, and O. D. Daraojimba, "Review of AI and machine learning applications to predict and thwart cyber-attacks in real-time," *Magna Scientia Adv. Res. Rev.*, vol. 10, no. 1, pp. 312–320, Feb. 2024.
[141] L. Chen, J. Liang, C. Wang, K. Yue, W. Li, and Z. Fu, "Adversarial attacks and adversarial training for burn image segmentation based on deep learning," *Med. Biol. Eng. Comput.*, vol. 62, no. 9, pp. 2717–2735, Sep. 2024.
[142] S. Xia, Y. Yu, X. Jiang, and H. Ding, "Mitigating the curse of dimensionality for certified robustness via dual randomized smoothing," 2024, *arXiv:2404.09586*.
[143] I. H. Sarker, H. Janicke, M. A. Ferrag, and A. Abuadbba, "Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions towards automation, intelligence and transparent cybersecurity modeling for critical infrastructures," *Internet Things*, vol. 25, Apr. 2024, Art. no. 101110.
[144] U. Schmid, "Trustworthy artificial intelligence: Comprehensible, transparent and correctable," in *Hannes Werthner Carlo Ghezzi Jeff Kramer Julian Nida-Rmelin Bashar Nuseibeh Erich Prem*, 2024, p. 151.
[145] S. Z. E. Mestari, G. Lenzini, and H. Demirci, "Preserving data privacy in machine learning systems," *Comput. Secur.*, vol. 137, Feb. 2024, Art. no. 103605.
[146] B. Dash and P. Sharma, "Are ChatGPT and deepfake algorithms endangering the cybersecurity industry? A review," *Int. J. Eng. Appl. Sci.*, vol. 10, no. 1, pp. 21–39, 2023.
[147] C. Eleftheriadis, A. Symeonidis, and P. Katsaros, "Adversarial robustness improvement for deep neural networks," *Mach. Vis. Appl.*, vol. 35, no. 3, p. 35, May 2024.
[148] L. Longo, M. Brcic, F. Cabitza, J. Choi, R. Confalonieri, J. D. Ser, R. Guidotti, Y. Hayashi, F. Herrera, A. Holzinger, R. Jiang, H. Khosravi, F. Lecue, G. Malgieri, A. Páez, W. Samek, J. Schneider, T. Speith, and S. Stumpf, "Explainable artificial intelligence (XAI) 2.0: A manifesto of open challenges and interdisciplinary research directions," *Inf. Fusion*, vol. 106, Jun. 2024, Art. no. 102301.
[149] C. Chakraborty, M. Bhattacharya, S. Pal, and S.-S. Lee, "From machine learning to deep learning: Advances of the recent data-driven paradigm shift in medicine and healthcare," *Current Res. Biotechnol.*, vol. 7, Nov. 2024, Art. no. 100164.
[150] D. Parikh, S. Radadia, and R. K. Eranna, "Privacy-preserving machine learning techniques, challenges and research directions," *Int. Res. J. Eng. Technol.*, vol. 11, no. 3, p. 499, 2024.

JIA YU received the Ph.D. degree in computer science from Northwestern Polytechnical University, Xi'an, China, in 2018. He was a Postdoctoral Researcher with the Software Research Institute (SRI), Technological University of the Shannon: Midlands, from 2022 to 2024. His research interests include computer security, audio content analysis, and natural language processing.

ALEXEY V. SHVETSOV received the Ph.D. degree from Russian University of Transport, Moscow, Russia, in 2018. He is currently an Associate Professor with the Department of Smart Technologies, Moscow Polytechnic University, and the Department of Operation of Road Transport and Car Service, North-Eastern Federal University. He has authored or coauthored more than 100 publications in refereed journals and conferences. His current research interest includes smart technologies.

SAEED HAMOOD ALSAMHI received the M.Tech. degree in communication systems and the Ph.D. degree from the Department of Electronics Engineering, Indian Institute of Technology (Banaras Hindu University)—IIT (BHU), Varanasi, India, in 2012 and 2015, respectively. In 2009, he was a Lecturer Assistant with the Engineering Faculty, IBB University, Ibb, Yemen. Afterward, he held a postdoctoral research position with the School of Aerospace Engineering, Tsinghua University, Beijing, China. Since 2019, he has been an Assistant Professor with Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen. In 2020, he was a MSCA Smart 4.0 Fellow with Athlone Institute of Technology, Athlone, Ireland. Currently, he is an Adjunct Professor with the Department of Computer Science and Engineering, College of Informatics, Korea University, Seongbuk-gu, Seoul, Republic of Korea; and an Assistant Professor with the Faculty of Engineering, IBB University. He has published more than 180 articles in high-reputation journals in IEEE, Elsevier, Springer, Wiley, and MDPI publishers. His research interests include green and semantic communication, green Internet of Things, QoE, QoS, Cybersecurity, multi-robot collaboration, blockchain technology, peatland and wastewater into energy, federated learning, and space technologies (high altitude platforms, drones, and tethered balloon technologies).