GLOBAL RESEARCH NETWORK

AMERICAN Journal of Engineering, Mechanics and Architecture
Volume 2, Issue 8, 2024 ISSN (E): 2993-2637

Security for Cyber-Physical Systems Using Machine Learning-Based Anomaly Detection: A Survey

Maytham Mohammed Tuaama
Imam Al-Kadhum College (IKC), Department of Computer Technical Engineering

Abstract: A Cyber-Physical System (CPS) is a hybrid system that uses both digital and physical parts. IoT, smart power grids and remote laboratory environments, online medical care, intelligent manufacturing, vehicles that are autonomous, the Internet of Things, control systems for industries, and many more have all contributed to CPS's explosive expansion over the last decade. Malicious attacks have increased dramatically due to the broad usage of Cyber-Physical Systems in modern life.

The increased access to the public internet has greatly increased the vulnerability of critical infrastructure, making incidents targeting oil pipelines and electrical power grids more prevalent and concerning. An extensive literature overview on recent developments in anomaly detection methods for Cyber-Physical System security threat identification is presented in this article. Within industrial control networks (ICS), resolving issues related to life safety is given top priority. Reading through a few articles allows us to spot trends and gaps in the literature. Resource limitations, there is a lack of established methods for communication, and the business is highly diverse, which makes it difficult to reach an agreement, and conflicting information security priorities between IT and OT networks are some of the significant outstanding issues highlighted in the article. Identifying possible answers and/or avenues for future study is done to address this.

Keywords: intrusion detection system; cyber-physical system; Anomaly Detection, IDS; CPS.

1. Introduction

The term cyber-physical systems (CPS) refers to those computer systems that interact with the physical world to control and monitor the behavior of physical entities, such as robots, drones, networks, power plants, water treatment facilities, and similar others [1]. The integration of sensor information with computational capabilities over the Internet of Things (IoT) is providing new opportunities for improved monitoring, management, and control of such systems. This has given rise to much research on many types of such CPS and corresponding analytic methods, along with rapid adoption of this new technology by industry [2]. IoT systems are enabling a level of physical awareness by the internet that is unparalleled in history [3]. However, the ability to control so many physical entities through the internet raises security concerns about the ability to prevent and detect electronic intrusions into cyber-physical systems. These electronic intrusions could have consequences that are potentially severe and, at times, even life-threatening [4]. Demonstrating their potential consequences, papers in the medical journals such as the Journal of the American Medical Association recently have investigated and reported on the effects of hacking into digital medical devices (a class of CPS) [5].

The need for secure control of CPS has long been recognized by the theoretical control community. Indeed, the foundational work in control theory area relies on the assumption that feedback can be done securely and that attackers cannot manipulate sensor measurements. Unfortunately, these assumptions do not always hold [6]. For example, the security threat caused by lightly protected civil infrastructure became a concern when the Stuxnet malware demonstrated the capability to control those facilities that were air-gapped from all networks except for those operated within the infrastructure community. Since then, there has been a growing number of cyber attacks and empirical reports on the security behaviors of many types of CPS [7]. These reports have made it clear that even traditional superiority-based relationships, such as those present in international relations, could be altered by the emergence of capabilities guided by cyber. To keep up with this new reality and to continue working toward vibrant and resilient electronic business and information, the area of industrial control in engineering is evolving from a working truth paradigm that the most technically efficient means of control is usually the most costly and secure alternative to emphasize the competence with which FAI could identify and hold insights from leading citizens [8], [9]. At the same time, in national security activities, early scientific research provides the initial experiment of the competition that terror organizations adapt to form the necessary human and technical control. Thus, the need for developing secure CPS and responding to crises that have arisen recently.

2. Fundamentals of Cyber-Physical Systems

2.1. Cyber-Physical Systems: Technologies and Challenges

The term cyber-physical systems is being increasingly used to describe systems that integrate communications, control, and computational techniques for system identification, design, and performance evaluation [10]. The technological advancements spurred by the virtual revolution have given us the flexibility to choose from hybrid cyber-physical systems when we design control systems. These systems are designed explicitly to exploit the advantages offered by networking, offering flexible designs that can be central (fully in software) or hierarchical [11]. An exemplary system is the smart grid, which will integrate generation, monitoring, distribution, and operating decision-making and may include renewable energy resources and electric vehicles. The central research questions that lie at the interface of physical system dynamics, cyber structures, and hybrid control systems are those related to designs that guarantee predictability, robustness, and, whenever possible, high performance [12]. These questions encompass areas such as optimal utilization of resources, efficient communication protocols, seamless integration of distributed components, and dynamic adaptability to changing operating conditions. Additionally, interdisciplinary collaboration plays a significant role in the development and advancement of cyber-physical systems. Researchers from various fields, including electrical engineering, computer science, mechanical engineering, and control systems engineering, work together to tackle the complex challenges and ensure the overall effectiveness and reliability of these systems [11]. Advancements in sensing technologies, data analytics, and machine learning have further expanded the capabilities and possibilities of cyber-physical systems. By leveraging these technologies, we can enhance system monitoring, fault detection, predictive maintenance, and decision-making processes. Furthermore, the integration of artificial intelligence and cognitive computing techniques enables cyber-physical systems to learn from past experiences, adapt to new situations, and optimize their performance continuously [2]. It is crucial to address security and privacy concerns in cyber-physical systems as well. As these systems become more interconnected and rely heavily on data exchange, protecting sensitive information and ensuring the integrity of the system is paramount. Robust authentication mechanisms, secure communication protocols, and encryption techniques are vital for safeguarding cyber-physical systems against malicious attacks and unauthorized access. The future of cyber-physical systems holds immense potential for transforming various domains, including transportation, healthcare, manufacturing, and infrastructure. With continued research and development efforts, we can further enhance the performance, efficiency, and reliability of these systems, ultimately leading to a more interconnected and intelligent world [13].

2.2. Fundamentals of Cyber-Physical Systems

All cyber-physical systems are characterized by significant computing and communication capabilities to achieve their physical system goals. These systems utilize smart sensor and actuator nodes with communication links in order to drive and observe physical processes [2]. Combination with networking technology greatly enhances the possibilities of cyber-physical systems, as showcased by the exponential growth of mobile computing and the global Internet [14]. As the demand for real-time distributed control, infobots, and telematics systems that control and inform people increases, there arises a need for more advanced system requirements that hardware alone cannot fulfill. Consequently, the research challenges mainly revolve around sensing, actuation, and computational technologies that can effectively support such integration [15]. The core computational system challenges lie in determining innovative approaches to achieve transformation or augmentation of perception or action in physical space using computer algorithms, as well as establishing robust networks with low bandwidth and energy consumption. Moreover, cyber-physical systems research at the hardware-software interface must also tackle dynamic system-level design issues, which are further complicated by constraints in energy and bandwidth [16]. This entails providing support for a diverse set of signal processing, communication, and control functionalities. Ultimately, addressing these intricate fundamental problems serves as the primary focus in the broader field of cyber-physical system research.

2.3. Security Challenges in Cyber-Physical Systems

Cyber-physical systems operate in complex, open, and unpredictable environments, and as a result, the security of these systems faces a new set of challenges. In this section, we provide a comprehensive review of the security challenges in each layer of the design stack including hardware security, network security, system software security, middleware security, and application security. In addition, We also cover the difficulties associated with ensuring the safety of some cyber-physical systems, such as self-driving cars, Industrial Internet of Things, smart grids, smart buildings, and flying ad hoc networks. Lastly, the increasing impact of social systems in cyber-physical systems calls for research into modeling and securing their impact. For each challenge, we provide a brief description and mention potential attack vectors.

Cyber-physical systems security is faced with new security challenges from both traditional computer systems and physical systems. Some of them, like performance and energy-efficient components (such as Field-Programmable Gate Arrays (FPGAs) or Graphics Processing Units (GPUs)), networked devices and multicore/multiprocessor architectures, I/O virtualization and security root of trust, have been well-studied [17]. However, advanced cyber-physical systems components bring security challenges difficult to handle. For instance, emerging non-volatile memory technology (like ReRAM, STT-MRAM, PCRAM) has various security vulnerabilities due to their unique properties [18], [19]. Long-range communication, collaboration, missions, and policies of devices have been associated with security issues [20]. The increasing number of on-chip cores aggravates the reliance on scaling hardware security primitives, such as processor and cache accesses, particularly used for secure encryption and authentication as well as Address Space Layout Randomization (ASLR) or key isolation [21]. A significant lack of physical security primitives has been observed. The cyber-physical systems must also preserve real-time guarantees, for example, delay sensitivity or being vulnerable to side-channel analysis [22].

2.3.1. Traditional Security Measures

With the rapid development of technology, there comes an increase in the ability for acts of sabotage against a system to become potentially more harmful. Therefore, the system must be both defensible and resilient when experiencing attacks or experiencing other types of faults, such as malfunctions of equipment. These types of systems are known as secure systems, which can be classified as traditional security measures, cryptographic measures, network layer measures, and conversion methods [23], [24].

Traditional security measures encompass security measures for critical systems from the physical world. Characteristics of these systems are: (i) the actions performed are tangible, (ii) can be operated as independent components, (iii) functions and structures are static, (iv) the input and output signals are digital [25], [26], [27].

The function of traditional measures is the control of functions of system resources. These techniques can be used in a variety of layers within the system, such as: (i) periphery sensors (usually have simple tasks), (ii) the inner system (have more complex tasks), (iii) interfaces between layers. Physical attacks are relatively simple and are a serious threat (such as accelerator injections and temperature alteration). Therefore, specific measures must be taken to reduce system vulnerability [28]

3. Cyber-Physical System Anomaly Detection

Cyber-physical systems (CPS) are the underlying technology of smart cities, smart grids, connected vehicles, and industrial control systems [29]. The security of CPS is becoming more and more important, as shown by increasing security incidents in recent years. Anomaly detection is usually the first step in security [30]. However, the security of CPS is very challenging.

First, compared to traditional computer systems, CPS is more complicated. It consists of both a cyber part and a physical part, which makes anomaly detection much more complicated [31].

Second, the normal situation in CPS can be more complicated than traditional computer systems. The traditional network packets and computing activities are now coupled with temperature, speed, position, and many other physical factors [32].

Third, attacks on CPS not only include damaging the computer system but also affecting the physical process through the computer system [28].

Finally, the complexity of the physical process and the requirement of real-time prediction mean that the machine learning models used need to be simple [33].

In this paper, we thoroughly examine and analyze the most recent and cutting-edge research that effectively combines the immense capabilities of machine learning with the field of cybersecurity, particularly when it comes to ensuring the security of cyber physical systems (CPS) on a practical and applicable scale. Our comprehensive review incorporates the latest overview work, carefully excluding studies that necessitate unrestricted access to data and fall outside the realm of computer science, especially in relation to Common Off The Shelf (COTS) firmware and the establishment of non-generalized trust boundaries. It is of utmost significance that our findings and insights are applicable to a diverse range of cyber physical systems, contributing to the advancement of CPS security. Figure (1) shows the types of anomalies in cyber-physical systems.

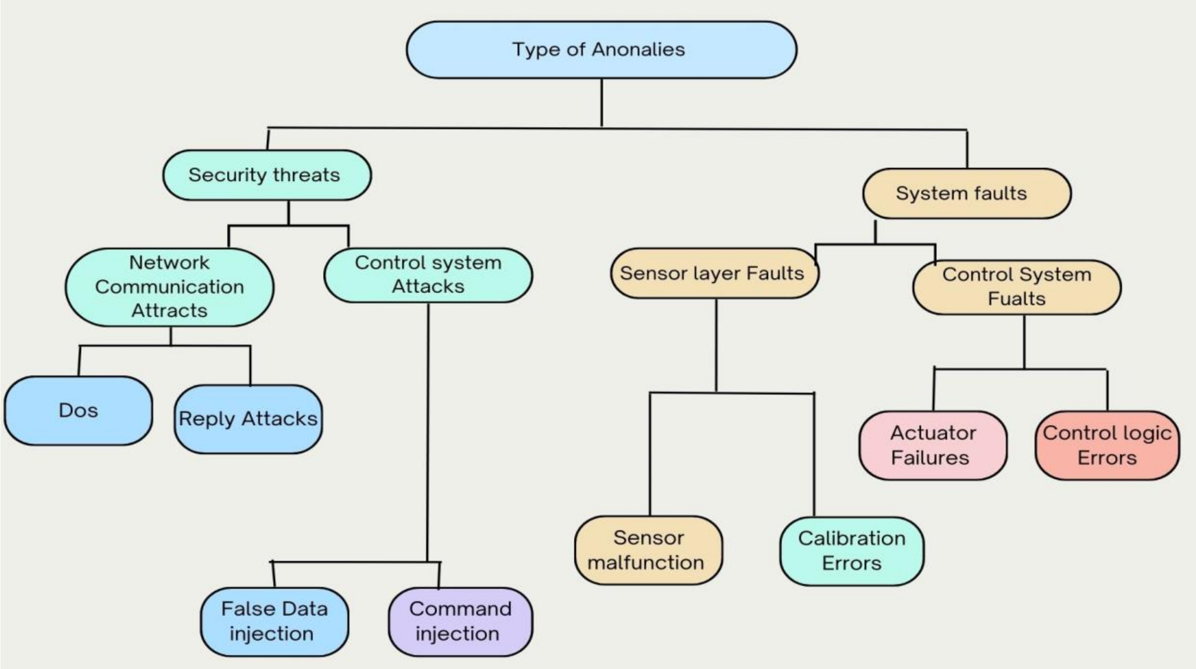

Fig (1) Type of Anomalies in cyber physical systems

3.1. Machine Learning Techniques

With the speed of hardware development and the increase in training data volume, machine learning (ML), especially deep learning (DL), now represents the cutting edge of anomaly detection. Another reason for the increased interest is the ability to abstract complex structures, which is essential to process high-dimensional sensor data [34]. One typical characteristic of ML-based AD is unsupervised learning, where model training does not require any labeled normal or abnormal data. When model training is finished, the model should be able to tell the difference between a normal and abnormal sample. This feature could automate model training without massive human effort as long as the AD model performs well [35].

Many ML techniques for AD are based on clustering algorithms, where K-means based algorithms like K-means and Fuzzy C-Means are used to divide the data set into K predefined clusters. During the model training phase, an auto-encoder based algorithm learns the manifold of the data set [36]. While the AD algorithm is effectively trained in an unsupervised way, it still suffers from huge human efforts. To remove the annotation burden, semi-supervised learning-based models, including long-short term memory (LSTM) based recurrent neural networks, sequence to sequence auto-encoder, and convolutional neural network (CNN)-based encoder and LSTM based decoder have been tried for the AD [37]. The unsupervised AD does not need to pre-train the deep neural networks. Different from the label unavailability in unsupervised AD, the goal of supervised AD is to classify normal or abnormalities after learning. Semi-supervised AD is a compromise, where the labeled data set has only a small fraction of the whole collection [38]. To effectively model the relationship among a bunch of sensors for sequential data, hybrid ML-based methods by combining symbolic query and model-based learning and LSTM with convolutional networks have been proposed for the construction of a multi-resolution spatio-temporal correlation [39]. The output of RNN networks is a latent distribution that encodes the data. A novel use regime for the variational autoencoder (VAE) assuming the conditional probability distribution of latent variables and the input data happens to satisfy the Gaussian distribution has also been studied [40]. The sudden change in the distribution properties could signal the existence of anomalies. Many other methods, for example, a neural network structured on a graph for semi-supervised classification and graph-based unsupervised anomaly detection, combining support vector machines with directed compounds, deep unsupervised learning for the unsupervised anomaly detection and feature importance guided data association have been proposed.

5. literature Analysis

Through the integration of computing and communication into physical processes, cyber-physical systems become useful tools for monitoring and controlling physical systems. [1]. However, resource-constrained cyber-physical systems and complex, environmentally varying working conditions make the control of and response to cyber-physical operations more difficult [41]. Traditional security methods can no longer fully meet the various threats to the security of cyber-physical systems. Anomaly detection methods, still, play an important role in the big families of security solutions for cyber-physical systems [42]. In this paper, we aim to provide a comprehensive analysis of how machine learning methods have been incorporated into anomaly detection in cyber-physical systems. Our study encompasses a wide range of disciplines, including machine learning, physical sciences, and various industries. By examining existing research and conducting experiments, we contribute to the current understanding of anomaly detection in cyber-physical systems. Furthermore, our survey focuses on the adaptivity of machine learning algorithms to complex and dynamic environments, ensuring their efficacy in real-world scenarios. We thoroughly investigate machine learning-based anomaly detection by analyzing diverse datasets with distinct characteristics, allowing us to establish quantitative and qualitative comparisons with benchmark datasets. Through our research, Our goal is to help improve cyber-physical system anomaly detection methods, addressing the ever-evolving challenges posed by the interplay between computation, communication, and physical processes.

This paper thoroughly investigates machine learning-based methods that can effectively integrate physical engineering concepts into small groups, thereby fostering innovation and advancement in this domain. To achieve this goal, benchmark datasets, meticulously chosen to represent the vast array of data collected from various computer systems pertaining to physical layer subjects, are employed [43], [44]. These heterogeneous benchmark datasets serve as a protective shield, enabling the presentation of multiple solutions based on the powerful radial basis function network approach applied to extensive multi-class physical industrial system datasets [45].

Moreover, a comprehensive performance experiment is meticulously conducted to examine the impact of feature dimension reduction on the system, utilizing the remarkable RBF convolution-based neural networks as classifiers [46], [47]. This experiment provides valuable insights and sheds light on the significance of feature dimension reduction in enhancing the overall performance and efficiency of the system.

The contributions presented in this paper are truly significant and add substantial value to the existing knowledge in this field. Firstly, a systematic literature survey is conducted, examining existing datasets and machine learning classifier methods specifically tailored for addressing physical conditions. This survey not only provides a comprehensive overview but also identifies gaps and opportunities for future research. Secondly, a novel and innovative implementation of feature dimension reduction for cyber-physical datasets is introduced, leveraging the powerful capabilities of RBF-CNNs. This implementation not only offers enhanced efficiency and accuracy but also adds a new dimension to the field of feature dimension reduction in cyber-physical systems.

Overall, this research paper serves as a comprehensive and essential resource for researchers, practitioners, and professionals working in the field of physical engineering, machine learning, and cyber-physical systems. The insights, methodologies, and findings presented in this paper lay a solid foundation for further advancements and discoveries, ultimately driving innovation and progress in this exciting and rapidly evolving field.

5.1. using IDS/IPS for Anomaly Detection

Intrusion Detection System (IDS) may be one of the most popular techniques for CPSoS anomaly detection [48]. It is widely deployed in various types of systems including e-commerce and telecommunication. Granville and Oliveira (2005) surveyed the various types of IDS [49], [50]. The Application IDS and Host IDS (HIDS) operate on individual servers. They collect information based on the complete list of system (or application) operations done periodically. This list of use of a system or application is made by listening all kernel calls triggered [51]. The External IDS (HIDS) works like the HIDS except that it listens to a network kernel call. The HIDS/external IDS enter in action only when something odd is occurring: unauthorized access which leads to a modification of the user list, sensor that had not to send an alert, messages that are attacks, etc [52], [53]. BaseStation, a system for monitoring wireless networks, uses a radio telescope approach wherein it listens to the entire band by receiving packets from the entire network. Each addressed packet is observed and is sent to the MIPS accelerator, where side-channel observations are compared to the model-based expectations. Packages found to be outliers are penalized and transmitted to the central server while the other packets are shuffled to the next simulation step [54].

The main problem of the IDS is its need to have static knowledge instead of learning [55]. An Intrusion Prevention System (IPS) signature is updated on an event basis, but for an IDS, the signature files must be downloaded and updated at regular intervals. The signature must be then installed on the routers or server, which may disrupt the CPSoS operation [56]. The activity of the IDS can also be the footprint of the use of an anomaly. But in the CPSoS, the update will be done on the fly during the execution of the model of the CPSoS adaptation, even when there is no anomaly [57]. Moreover, the knowledge of the IDS is specific to a technology, this technology being possibly very different between components of the CPSoS [58].

To compare the suggested method with similar approaches discovered in the literature, Table 1 provides a summarised summary of the key aspects. These characteristics are associated with (1) Method-implementation method of security;(2) Dataset-the dataset used with this algorithm;(3) Advantages & disadvantages of this model;(4) Contributions-the researcher's contributions in this article; and (5) Research Gap.

Sheng et.al. [59] provide a broader model that, by analyzing occurrences and patterns of node activity, may characterize the network in connection to both the natural environment and CPS processes. Anomaly events are defined as any behaviour that deviates from this model. Although existing intrusion detection systems (IDS) can spot suspicious activity, they are unable to provide any useful information on the total danger or its effects on the CPS. The proposed method worked well on publicly available datasets; however, when implemented in production systems, it generates many false positives.

Ravikumar et. al. [60] Within federated CPS settings, like networked smart electricity grids, build on Rakas's work by proposing a decentralized intrusion detection system (IDS). In order to gather information on network flows, this proposed distributed intrusion detection system mirrors the ports on Ethernet switches, and combine it in a centralised or cloud-based IDS environment. Its purpose is to enhance awareness of the situation of activities in a dispersed and/or loosely coupled CPS. Dynamically developing intrusion detection system (IDS) rules based on activity throughout a distributed or weakly linked IDS, such as a smart power grid, enables more robust safeguarding against cascade failures and quicker anomaly detection. Despite its impressive results on test datasets, it still needs more development to tackle the vastly more unpredictable real thing.

S. Seng et al. [61] focus on the large gap among academics with businesses in industrial network intrusion detection and prevention system design and operation. Attack detection in IT and OT networks has traditionally used signature-based methodologies. A database of hazardous patterns is used to identify malicious communications. An early and popular intrusion detection method is signature-based IDS. The signature database must be updated often since it misses new or zero-day attacks but detects old ones. Contrarily, anomaly-based detection uses AI and ML to model typical behavior and classify any variation as abnormal and harmful. Predetermined parameters for usual behavior are a basic anomaly-based detection method. The constraints of information technology networks apply to metrics like memory or processor consumption, while operational technology networks apply them to physical environmental parameters like voltage, pressure, temperature, etc.

Signature-based detection methods require regular database updates, but threshold-based detection strategies are accurate and require less system operator administrative effort to maintain the intrusion detection system. Low administrative requirements and high threat accuracy have made this type of intrusion detection system (IDS/IPS) popular in the business.

Khraisat et. al. [62] expand upon Seng's previous work by organizing existing intrusion detection and prevention systems (IDS/IPS) into a taxonomy and analyzing the various artificial intelligence (AI) and machine learning (ML) methods discussed in academic publications. The article presents a comprehensive analysis of various ML algorithms, outlining their pros and cons. The overarching idea is that an ensemble method, which integrates numerous ML algorithms, can achieve better results than any one algorithm could on its own. Industry adoption has been hindered by this method's increased complexity, which in turn requires extra time and skill from the system operator.

Vasan et. al. [63] Enhance Khraisat's ensemble learning model research to improve IIoT IDS and IPS accuracy. For Internet of Things (IoT) devices with limited processing power, a novel feature selection method that stacks diverse characteristics may reach 99.98% classification accuracy with reasonable computational overheads. Since bad actors are always enhancing their adversarial abilities, our ensemble learning method has concentrated on cross-platform malware. Internet of Things (IoT) assaults targeting diverse processor architectures have skyrocketed. Malware Threats Hunting utilizing Advanced Ensemble-Based Learning (MTHAEL) is a recommended ensemble model that trains a strong learner using weak learner algorithms to improve its predictions by combining their predictions.

MTHAEL disassembles IoT executable binary files to create a normal baseline. By studying OpCode instructions, which are machine code one step below assembly language, During normal functioning, we might be able to determine which operations took place. The interoperability of intrusion detection platforms in the vastly diverse IoT business is made possible by this incredibly low level of instruction. The main benefit of this technique is that it can use the same IDS and IPS across several IoT devices. This allows more users to use the IDS/IPS without modification, reducing the system operator's administrative workload. However, disassembling all software binaries is tedious and expert-intensive, prohibiting commercial usage outside of academia. SaaS is the best option to implement this intrusion detection system. This allows a centralized expert to use a federation dataset to swiftly detect known and unknown threats and maintain the IDS.

Abid et al. [64] propose a new approach to distributed intrusion detection systems (IDS) We may utilize machine learning to filter out malicious and recasting the challenges as big data, legitimate data from several sources, is consolidated in a cloud-based environment. Subsequently, we may instruct the dispersed node of the IDS to act upon the data that has been evaluated and categorized. The idea behind this approach is to improve the IDS's classification accuracy by feeding the ML model more comprehensive data sources than a single network viewpoint could supply. The vast diversity in IIoT designs means that this method, although helpful in a uniform IIoT setting, is mostly useless outside of a single company. This is in contrast to standard enterprise networks that use intrusion detection systems and firewalls; these networks are often more monocultural and can make better use of distributed learning models for these systems.

N Jeffrey et. al [65] to improve CPS safety, a hybrid anomaly detection model was suggested. The researcher delves into the topic of how the fast adoption of Industry 4.0 has led to the merging of IT and OT networks. Cyber-physical systems (CPS) are now more vulnerable to attacks because OT networks, which were once trusted and isolated, have converged with IT networks. There are major ramifications for the economy and security from these dangers. To effectively detect known threats in IT networks, this approach combines two types of Intrusion Detection Systems (IDS): signature-based and threshold-based. (ii)Machine learning (ML) techniques, built for OT networks specifically to detect abnormalities based on behavior. The goal of the hybrid approach is to improve the accuracy of unknown threat detection using behavior-based anomaly detection and to achieve faster detection of known threats. The hybrid model may struggle to adapt to new devices, communication protocols, or operational changes without major reconfiguration [31], despite the fact that this strategy tries to utilize the capabilities of each method. This is in contrast to scalability issues, where the CPS environment scales. As an alternative, security teams may find themselves under more operational pressure to continually update and fine-tune hybrid models that successfully integrate several detection methodologies [66].

TABLE 1

No	Author &year	Method	Dataset	Advantage	Disadvantage	contributions	Research Gap
48	Al-Mhiqani et.al 2024	SLR		the research provides classifications that help the reader understand different types of intrusion detection systems.	the study relied only on data found in the literature only	Giving a classification based on academic research, highlighting CPS insider threat detection methods and its subsections Highlighting CPS insider detection of threat study opportunities and challenges. This content may help readers understand CPS insider risk identification possibilities.	
52	JM Kizza 2024	ML tech	CSE-CIC-IDS2018	prevent unauthorized access and thus prevent system breaches	possibility of positive results	contribute to finding new ways to prevent and detect intrusions in maintaining network security.	Limitations facing network security in current hacks
53	Y.shen 2022	PKI model	NSL-KDD &UNSW-NB15	combine ML&DL models, improves speed and	new dataset may be suffering from inconsistency	novel dataset to address the obstacles of the older dataset	there is no dataset inclusive for everything

				accuracy for detecting cyber attacks.	and this could be another problem.		
54	S Chakaraborty et.al 2023	RFI	DSA-110	improve detection signal	Data Loss	framework for collaborative mitigation of RFI	impact on Data Quality
56	T Sommestad et.al 2022	Sonrt-NIDS	VRT	its specific identification for attack	false positive very high rate	help understand detection capabilities for signature-based NIDS	determine when signature-based attacks are well detected and under what circumstances they may fail.
57	R Pinto et.al 2022	A-HIDS	OPC UA network data	security enhancement	the requirements do not fully address for example knowledge security	state-of-the-art model Edge devices based IDS within CPPS	complexities of the Edge devices and difficulties of maintenance
59	C Sheng 2021	CP-SCADA	not detailed	combine network-level and physical-level modeling	implementation very complexity	provides novel methods for risk evaluation	integrating the physical level and network level
63	D Vasan et.al 2020	MTHAEL ARCHITECTURE	IOTcross-architecture dataset	the area of research is actively lead to novel data mining &DL method	the time of processing is very high	novel architecture MTHAEL	Real-time malware detection
64	A Abid et.al 2022	AI,Big Data techniques	SWaT	the accuracy is very high	implementation very complexity	novel model	Applications of Real-World
66	N Jeffrey et.al 2024	S-detection &Tdetection	new dataset	universal detection	complexity	novel hybrid detection model	challenging of combining IT&OT

5.2. using AI/ML to the detection of anomalies

With the development of deep learning in recent years, AI/ML has been widely applied in various disciplines, such as computer vision and natural language [67]. Its application benefits the operation of CPSs to some extent [68]. At the same time, cyber-attack technologies become more intelligent as well. For example, the state-of-the-art and cutting-edge cyber-attack technology includes GAN, transfer learning, and adversarial attack. These advanced technologies confound the development of defense capabilities [69], [70]. In contrast with expert knowledge-based cyber-attack detection, AI/ML-based cyber-attack detection has stronger data-driven capabilities, can capture the characteristics of cyber-attack traffic, has advantages in recognizing low-level attacks, and saves time and energy in the construction of specialized cyber-attack [71], [72]. Cyber-attack defense systems are developed rapidly based on AI/ML. Currently, AI/ML-based detection methods are generally divided into four categories: (1) classifier model-based, (2) unsupervised learning-based, (3) clustering-based, and (4) autoencoder-based [73], [74], [75].

For the purpose of comparison, Table 2 provides a brief summary of the key elements of the suggested solution and comparable approaches identified in the literature. These characteristics have a connection to: :(1) Method-implementation method of security;(2) Dataset-the dataset used with this algorithm;(3) Advantages & disadvantages of this model;(4)Contributions-the researcher contributions in this article; and (5) Research Gap.

Chen et al. [**76]**build upon existing GAN techniques, with an emphasis on malicious actors intentionally changing their payloads slightly to avoid detection by signature-based and behavior-based intrusion detection and prevention systems. Malware authors' evasive strategies have long been present in IT networks as polymorphic computer viruses, but signature-based detection technologies have typically been able to reduce their effects. For training detection techniques to identify malicious Internet traffic that has been purposefully blacked out to circumvent detection algorithms based on signature, the researcher, expand upon existing counter measures by using GAN approaches. This innovative method builds defenses against polymorphic attacks by training a machine learning model with a detailed description of all possible mutations of a specific harmful payload. The model mimics the techniques used by hostile actors.

Alsaedi et al. [77]One more encouraging ML approach for detecting intrusions is Long Short-Term Memory (LSTM). To identify harmful activity in CPS settings, the researcher present a new framework that trains a machine learning method to identify the predicted behaviour of a complex industrial network with several sensors using Deep Neural Networks (DNN). To improve prediction accuracy and reduce noise in complex datasetsIn order to capture long-term relationships, LSTM is employed as a model for temporal patterns using time-series data collected by sensors. Then, to hone in on the most important traits, it is mixed with a novel approach to using distinct weighting values.

Borcherding et al.[78] suggest an innovative approach that distinguishes between linear and non-linear ML models. It is believed that a linear paradigm of behaviors is less probable to learn feature dependencies, which is the basis of this technique. We may train linear models using optimised methods like Logistic Regression (LR) alongwith Support Vector Machine (SVM) by analysing statistics, and non-linear models with Neural Networks (NN) and Random Forest (RF) (RF). In the same way that ensemble learning combines many ML methods, this method chooses the optimal algorithm dynamically based on the dataset's contents.

Ha et al. [79] To address the problem of human comprehension, we propose an enhancement to the current One-Class Based Support Vector Machine (OCSVM) along with Long Short-Term Memory (LSTM) algorithms that incorporates XAI into the model. This enhancement will allow anomaly detection methods to reach predictive decisions in a human-readable manner. The CPS operator may save money on maintenance and utilize the embedded XAI modules to interpret the ML predictions, allowing for speedier decision-making that requires human participation. In the suggested architecture, data from streaming sensors feeds into an LStM autoencoder, which in turn undergoes further processing using OCSVM and is filtered by a XAI model that displays an explanation for abnormalities in a human-readable format. While LSTM excels with time-series data—which is a good fit for IIoT sensor data—its performance degrades when faced with massive datasets. To get over this issue, Ha et al. suggest using OCSVM to stream incoming sensor data. OCSVM is designed to quickly identify abnormal or normal data.

Huong et al. [80] core model known as FedEx. (Federation learning-based Explainable Anomaly Detection for the Industrial Control Systems) is fed by low-powered edge devices in an effort to improve XAI using federated learning. The current difficulties are approached as Big Data problems. In a geographically dispersed IIoT environment, data from less powerful sensor nodes is pre-processed on a moderately powerful edge node. After that, For further processing as well as model training, data is sent from every dispersed node on the edge to the more powerful central host. Thanks to federated learning, which enables remote nodes in a geographically dispersed environment to learn about localized zero-day threats, The distributed ICS can quickly detect anomalies in different regions of the world thanks to its two-stage processing. The two-stage approach, which optimizes the tradeoff between detection speed and accuracy, is made possible by strategically placing nodes at the edge that interact with the central federated learning system.

O.A.Ajala [81]The researcher suggests investigating the effectiveness of artificial intelligence (AI) and machine learning (ML) in enhancing cybersecurity, specifically focusing on anomaly detection, threat prediction, and automated response systems, in other words, Given the growing threat landscape, organizations need to develop and implement robust cybersecurity strategies. the integration of artificial intelligence (AI)and machine learning (ML) is becoming essential for improving threat detection, prediction, and automated response. AL/ML technologies can analyze vast datasets to identify patterns and predict potential threats, offering a pragmatic approach to enhancing cybersecurity defenses. the study examines successful AL/ML applications in cybersecurity, highlighting their benefits and challenges, in contrast, the drawbacks in two important points, **complexity:** AL/ML models require specialized knowledge for development and maintenance, posing a challenge for organizations lacking expertise. and **Data Privacy**: the collection and processing of large amounts of data may arise privacy concerns[82], [83].

Akinola el. al [84]This article explores using advanced AI techniques, including deep learning, unsupervised learning, and ensemble learning, to improve anomaly detection and threat management in cloud-connected medical systems. Traditional security methods are becoming less effective against modern cyberattacks, so AI/ML approaches are proposed to detect and mitigate threats more effectively. Techniques like adversarial machine learning and reinforcement learning allow systems to adapt to evolving threats, making AI/ML superior to traditional methods in identifying anomalies and defending against cyber threats. The integration of these techniques into healthcare systems will enhance security, protect patient data, and ensure the continuous operation of medical devices, ultimately improving patient safety and trust in healthcare services. However, finding several potential drawbacks associated with using AI/ML for cybersecurity in the context of the Internet of Medical Things (IoMT), **Vulnerability to Adversarial Attacks**: AI systems can be susceptible to adversarial attacks, where attackers manipulate inputs to deceive the AI, leading to incorrect or harmful actions [85]. **High Implementation Costs**: Developing and maintaining AI systems for cybersecurity can be expensive, requiring specialized expertise and resources that might not be available to all organizations[86].

TABLE 2

No	Author & year	Method	Dataset	Advantage	Disadvantage	contributions	Research Gap
70	Anita 2024	GAN	public space data	detection of zero-day - attack	cost very high & complexity	enhancing security & safety for robust protection	lack of app in public spaces for GAN
71	Umit et.al 2024	anomaly detection based on AI	PMU Data	enhancing efficiency &optimization	complexity management power system	implemented robust AI algorithm	challenge scalability
73	MM Saeed et.al 2023	FS tech	NSL-KDD & KDD Cup 1999	enhancing of detection zero-day attack	time-consuming	develop new method in IDS	combine AI with 6G security
74	O Akinola et.al 2024	AL/ML	healthcare data	efficiency improving	increasing security risks	develop ML tech to detect threats in real-time	identify threats in real-time in connection with medical

							devices
76	J Chen et.al 2020	GAN	ICS Dataset	increased strength against hostile attacks	overfitting & complexity in implementation	focus on several types of attacks	developing techniques that can protect against several threats
77	A Alsaedi2022	MCC &USMD framework	CPS Dataset	Enhancing the accuracy and reliability	the framework my have difficulty generalizing across different CPS environments, especially those with different sensor configurations and data characteristics	new method data-driven	detection threats in real-time
83	GS Nadella et.al 2024	LSTM, RNN, &MLP	Historical cyber attack data	improving of intrusion detection	difficult for scalability	combine AI in cyber security	analysis predictive in real-time
85	R Fulton et.al 2024	Risk-Benefit method	from several studies	universal framework	management complexity	novel AI R-Benefit model	proposed new framework
86	Taylor et.al 2024	case study	from several studies	Enhancing the trust of a customer	inadequate detection of sophisticated attacks	perception training	how effective is AI in cybersecurity

6. Conclusion and Future Directions

This article includes a comprehensive study on employing machine learning-based anomaly detection approaches in providing security for CPS. Leveraging the inherent ability of these approaches to model the complex relationships of features, an inductive transfer, empirical-based knowledge, and demonstrate robustness in the presence of changing, unexpected, networked scenarios, an objective lens is provided to facilitate a meaningful comparison considering different aspects. Practical and implementation issues are introduced, focusing on the applicability of anomaly detection under different types of threats and network configurations/traffic and technologies. A detailed experimental survey on performance benchmarking is offered to provide an understanding of the trade-offs between different approaches, considering their resources and costs. Finally, this survey presents a thorough discussion on the potential future research directions, gap areas, challenges, and untapped opportunities in the increasing prevalence of using machine learning algorithms in enabling robust anomaly-based protection mechanisms in different CPS configurations, from smart cities and industrial control systems to the transportation and electrical smart grid networks and intelligent interconnected devices and clinical health provider systems.

Bibliography:

1. G. Lampropoulos and K. Siakas, “Enhancing and securing cyber-physical systems and Industry 4.0 through digital twins: A critical review,” *Journal of software: evolution and process*, vol. 35, no. 7, p. e2494, 2023.
2. B. A. Salau, A. Rawal, and D. B. Rawat, “Recent advances in artificial intelligence for wireless internet of things and cyber–physical systems: A comprehensive survey,” *IEEE Internet Things J*, vol. 9, no. 15, pp. 12916–12930, 2022.

3. P. Marwedel, *Embedded system design: embedded systems foundations of cyber-physical systems, and the internet of things*. Springer Nature, 2021.
4. P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. Hong, "Internet of things: Evolution, concerns and security challenges," *Sensors*, vol. 21, no. 5, p. 1809, 2021.
5. A. J. Cartwright, "The elephant in the room: cybersecurity in healthcare," *J Clin Monit Comput*, vol. 37, no. 5, pp. 1123–1132, 2023.
6. G. Belgioioso *et al.*, "Online feedback equilibrium seeking," *IEEE Trans Automat Contr*, 2024.
7. A. A. Jamal, A.-A. M. Majid, A. Konev, T. Kosachenko, and A. Shelupanov, "A review on security analysis of cyber physical systems using Machine learning," *Mater Today Proc*, vol. 80, pp. 2302–2306, 2023.
8. O. E. Oluyisola, S. Bhalla, F. Sgarbossa, and J. O. Strandhagen, "Designing and developing smart production planning and control systems in the industry 4.0 era: a methodology and case study," *J Intell Manuf*, vol. 33, no. 1, pp. 311–332, 2022.
9. D. G. Broo, O. Kaynak, and S. M. Sait, "Rethinking engineering education at the age of industry 5.0," *J Ind Inf Integr*, vol. 25, p. 100311, 2022.
10. A. V. Jha *et al.*, "Smart grid cyber-physical systems: Communication technologies, standards and challenges," *Wireless Networks*, vol. 27, no. 4, pp. 2595–2613, 2021.
11. I. Horváth, "Designing next-generation cyber-physical systems: Why is it an issue?," *Journal of Integrated Design and Process Science*, vol. 26, no. 3–4, pp. 317–349, 2022.
12. R. Al-Ali, L. Bulej, J. Kofro\v{n}, and T. Bureš, "A guide to design uncertainty-aware self-adaptive components in cyber–physical systems," *Future Generation Computer Systems*, vol. 128, pp. 466–489, 2022.
13. M. Hamzah *et al.*, "Distributed Control of Cyber Physical System on Various Domains: A Critical Review," *Systems*, vol. 11, no. 4, p. 208, 2023.
14. S. Gaba, I. Budhiraja, V. Kumar, and A. Makkar, "Advancements in enhancing cyber-physical system security: Practical deep learning solutions for network traffic classification and integration with security technologies," *Mathematical Biosciences and Engineering*, vol. 21, no. 1, pp. 1527–1553, 2024.
15. D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," *Comput Secur*, vol. 89, p. 101677, 2020.
16. A. Barišić *et al.*, "Multi-paradigm modeling for cyber–physical systems: A systematic mapping review," *Journal of Systems and Software*, vol. 183, p. 111081, 2022.
17. Z. Yu, H. Gao, X. Cong, N. Wu, and H. H. Song, "A Survey on Cyber–Physical Systems Security," *IEEE Internet Things J*, vol. 10, no. 24, pp. 21670–21686, 2023.
18. A. Yusuf, T. Adegbija, and D. Gajaria, "Domain-Specific STT-MRAM-based In-Memory Computing: A Survey," *IEEE Access*, 2024.
19. B. Prasad, S. Parkin, T. Prodromakis, C.-B. Eom, J. Sort, and J. L. MacManus-Driscoll, "Material challenges for nonvolatile memory," *APL Mater*, vol. 10, no. 9, 2022.
20. M. Dansarie, "Security Issues in Special-Purpose Digital Radio Communication Systems: A Systematic Review," *IEEE Access*, 2024.
21. W. Guo, S. Lian, C. Dong, Z. Chen, and X. Huang, "A survey on security of digital microfluidic biochips: Technology, attack, and defense," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 27, no. 4, pp. 1–33, 2022.

22. Y. Wang, A. Li, J. Wang, S. Baruah, and N. Zhang, “Opportunistic Data Flow Integrity for Real-time Cyber-physical Systems Using Worst Case Execution Time Reservation,” in *Proceedings of the 33rd USENIX Conference on Security Symposium*, 2024.

23. A. Shapiro, “Platform sabotage,” *J Cult Econ*, vol. 16, no. 2, pp. 203–220, 2023.

24. D. Sharapov and S. C. MacAulay, “Design as an isolating mechanism for capturing value from innovation: From cloaks and traps to sabotage,” *Academy of Management Review*, vol. 47, no. 1, pp. 139–161, 2022.

25. S. Rangaraju, “Secure by intelligence: enhancing products with AI-driven security measures,” *EPH-International Journal of Science And Engineering*, vol. 9, no. 3, pp. 36–41, 2023.

26. M. Abdel-Rahman and others, “Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world,” *Eigenpub Review of Science and Technology*, vol. 7, no. 1, pp. 138–158, 2023.

27. B. Ojo, J. C. Ogborigbo, and M. O. Okafor, “Innovative solutions for critical infrastructure resilience against cyber-physical attacks,” 2024.

28. W. Duo, M. Zhou, and A. Abusorrah, “A survey of cyber attacks on cyber physical systems: Recent advances and challenges,” *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 5, pp. 784–800, 2022.

29. A. Pundir, S. Singh, M. Kumar, A. Bafila, and G. J. Saxena, “Cyber-physical systems enabled transport networks in smart cities: Challenges and enabling technologies of the new mobility era,” *IEEE Access*, vol. 10, pp. 16350–16364, 2022.

30. S. M. Nagarajan, G. G. Deverajan, A. K. Bashir, R. P. Mahapatra, and M. S. Al-Numay, “IADF-CPS: Intelligent anomaly detection framework towards cyber physical systems,” *Comput Commun*, vol. 188, pp. 81–89, 2022.

31. N. Jeffrey, Q. Tan, and J. R. Villar, “A Review of Anomaly Detection Strategies to Detect Threats to Cyber-Physical Systems,” *Electronics (Basel)*, vol. 12, no. 15, p. 3283, 2023.

32. M. K. Habib, C. Chimsom, and others, “CPS: Role, characteristics, architectures and future potentials,” *Procedia Comput Sci*, vol. 200, pp. 1347–1358, 2022.

33. C. Lv *et al.*, “Machine learning: an advanced platform for materials development and state prediction in lithium-ion batteries,” *Advanced Materials*, vol. 34, no. 25, p. 2101474, 2022.

34. M. Bahri, F. Salutari, A. Putina, and M. Sozio, “AutoML: state of the art with a focus on anomaly detection, challenges, and research directions,” *Int J Data Sci Anal*, vol. 14, no. 2, pp. 113–126, 2022.

35. S. Zehra *et al.*, “Machine learning-based anomaly detection in NFV: A comprehensive survey,” *Sensors*, vol. 23, no. 11, p. 5340, 2023.

36. Z. Huang, H. Zheng, C. Li, and C. Che, “Application of machine learning-based k-means clustering for financial fraud detection,” *Academic Journal of Science and Technology*, vol. 10, no. 1, pp. 33–39, 2024.

37. P. S. Muhuri, P. Chatterjee, X. Yuan, K. Roy, and A. Esterline, “Using a long short-term memory recurrent neural network (LSTM-RNN) to classify network attacks,” *Information*, vol. 11, no. 5, p. 243, 2020.

38. L. Heckler, R. König, and P. Bergmann, “Exploring the importance of pretrained feature extractors for unsupervised anomaly detection and localization,” in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2023, pp. 2917–2926.

39. S. C. K. Tekouabou, E. B. Diop, R. Azmi, R. Jaligot, and J. Chenal, “Reviewing the application of machine learning methods to model urban form indicators in planning decision

support systems: Potential, issues and challenges," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 8, pp. 5943–5967, 2022.

40. N. Nguyen and B. Quanz, "Temporal latent auto-encoder: A method for probabilistic multivariate time series forecasting," in *Proceedings of the AAAI conference on artificial intelligence*, 2021, pp. 9117–9125.
41. A. Puliafito, G. Tricomi, A. Zafeiropoulos, and S. Papavassiliou, "Smart cities of the future as cyber physical systems: Challenges and enabling technologies," *Sensors*, vol. 21, no. 10, p. 3349, 2021.
42. V. V. Vegesna, "Machine Learning Approaches for Anomaly Detection in Cyber-Physical Systems: A Case Study in Critical Infrastructure Protection," *International Journal of Machine Learning and Artificial Intelligence*, vol. 5, no. 5, pp. 1–13, 2024.
43. M. Akrout, A. Feriani, F. Bellili, A. Mezghani, and E. Hossain, "Domain generalization in machine learning models for wireless communications: Concepts, state-of-the-art, and open issues," *IEEE Communications Surveys & Tutorials*, 2023.
44. B. Ozpoyraz, A. T. Dogukan, Y. Gevez, U. Altun, and E. Basar, "Deep learning-aided 6G wireless networks: A comprehensive survey of revolutionary PHY architectures," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 1749–1809, 2022.
45. J. Long, Y. Qin, Z. Yang, Y. Huang, and C. Li, "Discriminative feature learning using a multiscale convolutional capsule network from attitude data for fault diagnosis of industrial robots," *Mech Syst Signal Process*, vol. 182, p. 109569, 2023.
46. C.-H. Loh, Y.-C. Chen, and C.-T. Su, "Using Transfer Learning and Radial Basis Function Deep Neural Network Feature Extraction to Upgrade Existing Product Fault Detection Systems for Industry 4.0: A Case Study of a Spring Factory," *Applied Sciences*, vol. 14, no. 7, p. 2913, 2024.
47. S. Cong and Y. Zhou, "A review of convolutional neural network architectures and their optimizations," *Artif Intell Rev*, vol. 56, no. 3, pp. 1905–1969, 2023.
48. M. N. Al-Mhiqani, T. Alsboui, T. Al-Shehari, K. hameed Abdulkareem, R. Ahmad, and M. A. Mohammed, "Insider threat detection in cyber-physical systems: a systematic literature review," *Computers and Electrical Engineering*, vol. 119, p. 109489, 2024.
49. P. Shukla, C. R. Krishna, and N. V. Patil, "Iot traffic-based DDoS attacks detection mechanisms: A comprehensive review," *J Supercomput*, vol. 80, no. 7, pp. 9986–10043, 2024.
50. S. Nicolazzo, A. Nocera, and W. Pedrycz, "Service Level Agreements and Security SLA: A Comprehensive Survey," *arXiv preprint arXiv:2405.00009*, 2024.
51. R. Mitev, A. Pazii, M. Miettinen, W. Enck, and A.-R. Sadeghi, "Leakypick: Iot audio spy detector," in *Proceedings of the 36th Annual Computer Security Applications Conference*, 2020, pp. 694–705.
52. J. M. Kizza, "System intrusion detection and prevention," in *Guide to computer network security*, Springer, 2024, pp. 295–323.
53. Y. Shen, "Machine Learning and Knowledge-Based Integrated Intrusion Detection Schemes," Université d'Ottawa/University of Ottawa, 2022.
54. S. Chakraborty, G. Hellbourg, M. Careem, D. Saha, and A. Dutta, "Collaboration with Cellular Networks for RFI Cancellation at Radio Telescope," *IEEE Trans Cogn Commun Netw*, vol. 9, no. 3, pp. 765–778, 2023.
55. A. Thakkar and R. Lohiya, "A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions," *Artif Intell Rev*, vol. 55, no. 1, pp. 453–563, 2022.

56. T. Sommestad, H. Holm, and D. Steinvall, “Variables influencing the effectiveness of signature-based network intrusion detection systems,” *Information security journal: a global perspective*, vol. 31, no. 6, pp. 711–728, 2022.

57. R. Pinto, G. Gonçalves, J. Delsing, and E. Tovar, “Enabling data-driven anomaly detection by design in cyber-physical production systems,” *Cybersecurity*, vol. 5, no. 1, p. 9, 2022.

58. S. N. M. Garc\'\ia, A. Sánchez-Cabrera, E. Schiavone, and A. Skarmeta, “Integrating the manufacturer usage description standard in the modelling of cyber–physical systems,” *Comput Stand Interfaces*, vol. 87, p. 103777, 2024.

59. C. Sheng, Y. Yao, Q. Fu, and W. Yang, “A cyber-physical model for SCADA system and its intrusion detection,” *Computer Networks*, vol. 185, p. 107677, 2021, doi: https://doi.org/10.1016/j.comnet.2020.107677.

60. G. Ravikumar, A. Singh, J. R. Babu, A. Moataz A, and M. Govindarasu, “D-IDS for Cyber-Physical DER Modbus System - Architecture, Modeling, Testbed-based Evaluation,” in *2020 Resilience Week (RWS)*, 2020, pp. 153–159. doi: 10.1109/RWS50334.2020.9241259.

61. S. Seng, J. Garcia-Alfaro, and Y. Laarouchi, “Why anomaly-based intrusion detection systems have not yet conquered the industrial market?,” in *International Symposium on Foundations and Practice of Security*, 2021, pp. 341–354.

62. A. Khraisat and A. Alazab, “A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges,” *Cybersecurity*, vol. 4, pp. 1–27, 2021.

63. D. Vasan, M. Alazab, S. Venkatraman, J. Akram, and Z. Qin, “MTHAEL: Cross-architecture IoT malware detection based on neural network advanced ensemble learning,” *IEEE Transactions on Computers*, vol. 69, no. 11, pp. 1654–1667, 2020.

64. A. Abid, F. Jemili, and O. Korbaa, “Distributed architecture of an intrusion detection system in industrial control systems,” in *International Conference on Computational Collective Intelligence*, 2022, pp. 472–484.

65. N. Jeffrey, Q. Tan, and J. R. Villar, “A hybrid methodology for anomaly detection in Cyber–Physical Systems,” *Neurocomputing*, vol. 568, p. 127068, 2024.

66. G. Sebestyen and A. Hangan, “Anomaly detection techniques in cyber-physical systems,” *Acta Universitatis Sapientiae, Informatica*, vol. 9, no. 2, pp. 101–118, 2017.

67. A. T. G. Tapeh and M. Z. Naser, “Artificial intelligence, machine learning, and deep learning in structural engineering: a scientometrics review of trends and best practices,” *Archives of Computational Methods in Engineering*, vol. 30, no. 1, pp. 115–159, 2023.

68. B. A. Yilma, H. Panetto, and Y. Naudet, “Systemic formalisation of Cyber-Physical-Social System (CPSS): A systematic literature review,” *Comput Ind*, vol. 129, p. 103458, 2021.

69. M. Mashrur Arifin, M. Shoaib Ahmed, T. K. Ghosh, J. Zhuang, and J. Yeh, “A Survey on the Application of Generative Adversarial Networks in Cybersecurity: Prospective, Direction and Open Research Scopes,” *arXiv e-prints*, p. arXiv–2407, 2024.

70. A. Chaudhary, “Innovative Approaches to Public Safety: Implementing Generative Adversarial Networks (GANs) for Cyber Security Enhancement in Public Spaces,” in *Enhancing Security in Public Spaces Through Generative Adversarial Networks (GANs)*, IGI Global, 2024, pp. 296–304.

71. U. Cali, F. O. Catak, and U. Halden, “Trustworthy cyber-physical power systems using AI: dueling algorithms for PMU anomaly detection and cybersecurity,” *Artif Intell Rev*, vol. 57, no. 7, p. 183, 2024.

72. L. Yang, M. El Rajab, A. Shami, and S. Muhaidat, “Diving Into Zero-Touch Network Security: Use-Case Driven Analysis,” *Authorea Preprints*, 2023.

73. M. M. Saeed, R. A. Saeed, M. Abdelhaq, R. Alsaqour, M. K. Hasan, and R. A. Mokhtar, “Anomaly detection in 6G networks using machine learning methods,” *Electronics (Basel)*, vol. 12, no. 15, p. 3300, 2023.

74. O. Akinola *et al.*, “Artificial Intelligence and Machine Learning Techniques for Anomaly Detection and Threat Mitigation in Cloud-Connected Medical Devices,” *International Journal of Scientific Research and Modern Technology*, vol. 3, no. 3, 2024.

75. M. Nuaimi, L. C. Fourati, and B. Ben Hamed, “Intelligent approaches toward intrusion detection systems for Industrial Internet of Things: A systematic comprehensive review,” *Journal of Network and Computer Applications*, vol. 215, p. 103637, 2023.

76. J. Chen, X. Gao, R. Deng, Y. He, C. Fang, and P. Cheng, “Generating adversarial examples against machine learning-based intrusion detector in industrial control systems,” *IEEE Trans Dependable Secure Comput*, vol. 19, no. 3, pp. 1810–1825, 2020.

77. A. Alsaedi, Z. Tari, R. Mahmud, N. Moustafa, A. Mahmood, and A. Anwar, “USMD: UnSupervised Misbehaviour Detection for Multi-Sensor Data,” *IEEE Trans Dependable Secure Comput*, vol. 20, no. 1, pp. 724–739, 2023, doi: 10.1109/TDSC.2022.3143493.

78. A. Borcherding, L. Feldmann, M. Karch, A. Meshram, and J. Beyerer, “Towards a Better Understanding of Machine Learning based Network Intrusion Detection Systems in Industrial Networks.,” in *ICISSP*, 2022, pp. 314–325.

79. N. X. Hoang, N. V. Hoang, N. H. Du, T. T. Huong, K. P. Tran, and others, “Explainable anomaly detection for industrial control system cybersecurity,” *IFAC-PapersOnLine*, vol. 55, no. 10, pp. 1183–1188, 2022.

80. T. T. Huong *et al.*, “Federated learning-based explainable anomaly detection for industrial control systems,” *IEEE Access*, vol. 10, pp. 53854–53872, 2022.

81. O. A. Ajala, “Leveraging AI/ML for anomaly detection, threat prediction, and automated response.,” 2024.

82. 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 Journal of Advanced Research and Reviews*, vol. 21, no. 1, pp. 2286–2295, 2024.

83. G. S. Nadella and H. Gonaygunta, “Enhancing Cybersecurity with Artificial Intelligence: Predictive Techniques and Challenges in the Age of IoT,” *International Journal of Science and Engineering Applications*, vol. 13, no. 04, pp. 30–33, 2024.

84. O. Akinola *et al.*, “Artificial Intelligence and Machine Learning Techniques for Anomaly Detection and Threat Mitigation in Cloud-Connected Medical Devices,” *International Journal of Scientific Research and Modern Technology*, vol. 3, no. 3, 2024.

85. R. Fulton, D. Fulton, N. Hayes, and S. Kaplan, “The Transformation Risk-Benefit Model of Artificial Intelligence: Balancing Risks and Benefits Through Practical Solutions and Use Cases,” *arXiv preprint arXiv:2406.11863*, 2024.

86. K. AL-Dosari, N. Fetais, and M. Kucukvar, “Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges,” *Cybern Syst*, vol. 55, no. 2, pp. 302–330, 2024