



A Systematic Mapping Study and Empirical Comparison of Data-Driven Intrusion Detection Techniques in Industrial Control Networks

Bayu Adhi Tama¹ · Soo Young Lee² · Seungchul Lee^{2,3,4}

Received: 4 December 2020 / Accepted: 7 May 2022 / Published online: 29 May 2022
© The Author(s) 2022

Abstract

A rising communication between modern industrial control infrastructure and the external Internet worldwide has led to a critical need to secure the network from multifarious cyberattacks. An intrusion detection system (IDS) is a preventive mechanism where new sorts of hazardous threats and malicious activities could be detected before harming the industrial process's critical infrastructure. This study reviews the cutting-edge technology of artificial intelligence in developing IDS in industrial control networks by carrying out a systematic mapping study. We included 74 foremost publications from the current literature. These chosen publications were grouped following the types of learning tasks, i.e., supervised, unsupervised, and semi-supervised. This review article helps researchers understand the present status of artificial intelligence techniques applied to IDS in industrial control networks. Other mapping categories were also covered, including year published, publication venues, dataset considered, and IDS approaches. This study reports an empirical assessment of several classification algorithms such as random forest, gradient boosting machine, extreme gradient boosting machine, deep neural network, and stacked generalization ensemble. Statistical significance tests were also used to assess the classifiers' performance differences in multiple scenarios and datasets. This paper provides a contemporary systematic mapping study and empirical evaluation of IDS approaches in industrial control networks.

1 Introduction

An *industrial control network* is a collection of interconnected devices that are responsible for managing and monitoring physical equipment in the industrial domain [1]. Through the fast-developing of information and communication technology, manual labors, undoubtedly, has been substituted by more reliable automated equipment, enabling better production monitoring and quality control in industry operations. As a result, efficient communication to connect the whole equipment is desirable, leading to the penetration

of the communication networks into industrial segments. Industrial control networks; we hereafter refer them as industrial control systems (ICSs), might be decomposed into three main components, such as programmable logic controllers (PLCs), supervisory control, and data acquisition (SCADA), and distributed control systems (DCSs) [2]. In the past, ICS networks were mainly tangibly independent from outside networks due to the lack of communication protocols. Reasoning from this fact, today's ICSs are massively connected with external networks, including the Internet of Things (IoT) platforms that allow low-cost productivity and improved performance [3, 4]. However, this remains a problem concerning security since ICSs are prone to cyberattacks that might arise from internal and external networks [5, 6].

A multifariousness of cybersecurity attacks of ICSs has attained an ever-growing awareness due to a considerable rise in the number of security accidents in ICSs currently, which indicates a severe infrastructure susceptibility [7]. Moreover, since ICSs consist of some critical facilities, i.e., nuclear plants, power grid, and other industrial control systems, insecure infrastructure, and unqualified industrial networks might put industries at huge financial risk [8]. A successful attack on an ICS would severely harm any industry.

✉ Seungchul Lee
seunglee@postech.ac.kr

¹ Data Science Group, Institute for Basic Science (IBS),
Daejeon 34126, Republic of Korea

² Department of Mechanical Engineering, POSTECH,
Pohang-si 37673, Republic of Korea

³ Graduate School of Artificial Intelligence, POSTECH,
Pohang-si 37673, Republic of Korea

⁴ Institute for Convergence Research and Education
in Advanced Technology, Yonsei University, 50, Yonsei-ro,
Seodaemun-gu, Seoul 03722, Republic of Korea

Negative consequences include financial loss, operational failure, damaged equipment, industrial property piracy, and significant safety risk. The configuration and scale of an ICS will determine whether or not it has faults. The larger the system, the bigger the chance for attackers to exploit. An ICS that installs its former system with advanced tools, e.g., Industrial Internet of Things (IIoT), might have more specific threats and security risks. Hence, security protection and mitigation strategies of the relevant ICSs are a must [9].

A strategy for addressing the issues mentioned above is to develop intrusion detection systems (IDSs). An IDS includes one of the prevention mechanisms used to eliminate unauthorized activities within a system network due to ICSs software vulnerabilities. It aims at detecting and intercepting the attacks automatically by analyzing network and file access logs, audit trails, and other relevant information in a computer system [10, 11]. Since the earliest IDS concept introduced by Anderson [12], there has been a considerable increase in research interest to implement intrusion detection technology for ICSs. Artificial intelligence (AI) techniques, e.g., machine learning and deep learning algorithms, have been utilized to ameliorate the performance of IDSs [13]. Sort of IIoT devices might produce large amounts of data from a sensor, machine-to-machine (M2M) communication, and automation. This paradigm has shifted the research direction from a traditional data analysis using shallow machine learning (ML) to a big data analysis using deep learning (DL) techniques [14].

In addition, because of the ever-increasing complexity of ICSs, the conventional intrusion detection systems in the information technology domain are not fit to industrial process [15], it thus has rendered DL-based intrusion detection techniques fascinating. This study presents a systematic review of state-of-the-art artificial intelligence techniques used for intrusion detection/prevention in ICSs. The study has been extended to include DL algorithms, such as deep neural network (DNN), convolutional neural network (CNN), and recurrent neural network (RNN), providing researchers and practitioners an insight into the current status and future trends of IDSs literature adopted in the ICSs environment.

The remainder of the paper is structured as follows. Section 2 discusses the basic concepts of industrial control and intrusion detection systems. Section 3 substantiates the current research by comparing it to several similar survey studies, whereas Sect. 4 details the mapping study methodology. Section 5 summarizes and explains the results from the mapping study for each category. Section 6 examines several methods for implementing IDSs in ICSs, followed by Sect. 7, which includes the concluding observations and discusses the future research directions.

2 Background

2.1 Industrial Control Systems

An ICS can be viewed as interconnected devices, systems, networks, and controls utilized to automatize industrial processes [16]. Each ICS operates in several ways to handle the tasks depending on the type of industry efficiently. The devices and protocols in an ICS are utilized as the backbone in almost all industrial sectors and major facilities, providing infrastructures for electricity generation and distribution, water treatment and supply, manufacturing, and transportation.

ICSs lay down in several variants, more typical of which are SCADA, DCSs, and PLCs. Nevertheless, the contrasts and boundaries between these categories are not consistently figured out. Determining apparent differences can be no less strict due to the advancement of technologies used by these categories. SCADA systems are primarily employed for the acquisition and processing of a large amount of data and control industrial equipment by establishing remote commands [1, 18]. DCSs consist of multiple local controllers that are managed by a centralized supervisory control loop. PLCs are digital computer apparatus that takes inputs from data generation means, e.g., sensors, transmit them to the whole production units, and provide the outputs through human-machine interfaces.

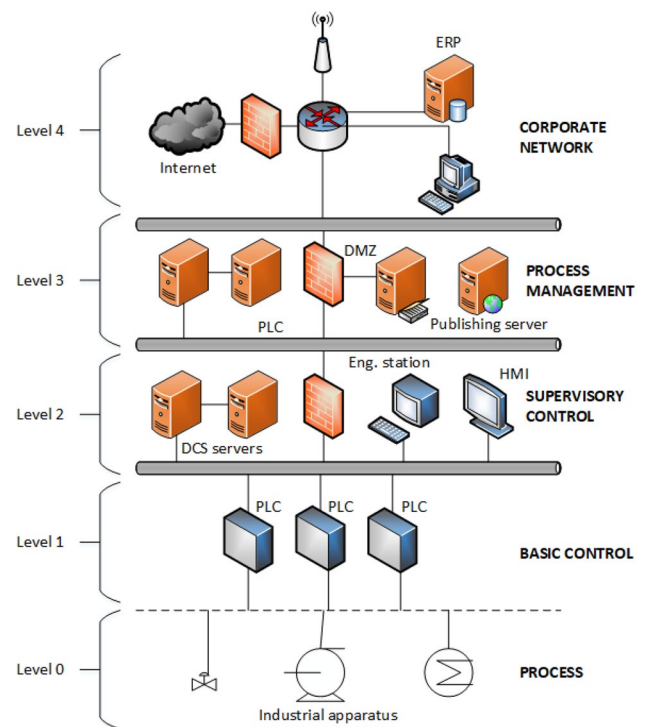


Fig. 1 A multi-level ICSs architecture [17]

An ICS is composed of multi-level architecture (see Fig. 1). *Level 0* forms the system's front-line, where industrial physical components and their related instrumentation are organized. The devices can be actuators and sensors that involve in performing diagnostic operations and communicating with other components. The aim of *Level 1* is to control and manage the industrial process using controller devices, e.g., PLCs. Concerning structure, PLCs are composed of some computing devices, i.e., CPU, RAM, input/output modules, and communication interfaces that allow real-time communication with sensors and actuators [19]. *Level 2* involves some control servers responsible for collecting information from the lower layers used to monitor and diagnostic purposes. Next, the collected information is presented to the operators via a human-machine interface (HMI), a graphical indicator that provides the physical process's circumstance. Lastly, *Level 3-4* incorporates the allocation and optimization resources, maintenance planning, and quality control. These actions are planned based on the information collected from the previous stages.

As compared to prevalent information technology (IT) systems, ICSs have some specific characteristics that must be taken into consideration. Some primary differences should not be omitted while considering security measures within industrial control ecosystem. Table 1 outlines some key distinctions between conventional IT systems and ICSs [1, 16, 20].

2.2 Intrusion Detection Systems

An *intrusion detection system* is a responsive security mechanism used to monitor the network security status by detecting external aggression and anomalous servers' operations. It aims at providing credible traces of information systems being intruded. Concerning the detection approach, an IDS

might have two distinct categories, i.e., anomaly-based and misuse-based. The former approaches assume that an intruder can be detected by inspecting deviations from the regular network traffic. An advantage of these approaches includes the ability to detect unacknowledged attacks; however, they remain to suffer from a considerable amount of false alarm rate [22–24]. On the other hand, the latter [25] works based on some known attack signatures, in which a possible attack is analyzed and detected by comparing it with such pre-defined attack signatures provided by a knowledge base of attack. A pattern-matching approach is commonly utilized in the suspicious detection task. In contrast to anomaly-based IDSs, misuse-based IDSs generate a lower false alarm rate, yet, unknown attack detection is lacking.

Additionally, IDSs can be classified into two primary deployment types, namely host-based and network-based. The primary objective of host-based intrusion detection systems (HIDSs) is to monitor and then notify about occurrences on a local computer system. A hash of the file system is one example found in HIDS. Untrustworthy behavior is identified by comparing the differences between the recalculated hash value and the previously saved in the database. On the other hand, network-based intrusion detection systems (NIDS) are intended to monitor network traffic and detect malicious activity by examining inbound network packets. To summarize, Fig. 2 illustrates the breadth of IDSs discussed in [21].

3 Problem Definition and Motivation

Most previous research concentrates on machine learning, deep learning, and intrusion detection in industrial control systems. Some surveys have either emphasized machine learning algorithms [26–29], intrusion detection

Table 1 The distinctions between conventional IT systems and ICSs

Category	Conventional IT systems	Industrial control systems
Performance and timeliness	Response time is less critical, <i>jitter</i> is only essential in VoIP	Real-time and deterministic
Availability	Less important	High degree, i.e. unpredictable failure is intolerable
Resource constraints	Abundant	Limited to specific embedded devices such as controllers
Component lifetime	3–5 years	15–20 years
Risk management	Data confidentiality and integrity	Human safety and regulatory compliance
System operation	Typical	Proprietary
Communications	Standard	Proprietary
Component location	Local and easy to access	Isolated and remote
Managed support	Diverse	Single vendor
Change management	Timely fashion, or automated	Thorough test, outage is planned
User	Person	Computer or highly intelligent control device
Nature of system	Centralized to lower operational costs	Distributed to insure reliability and availability
Security focus	Encryption algorithm	VPN security

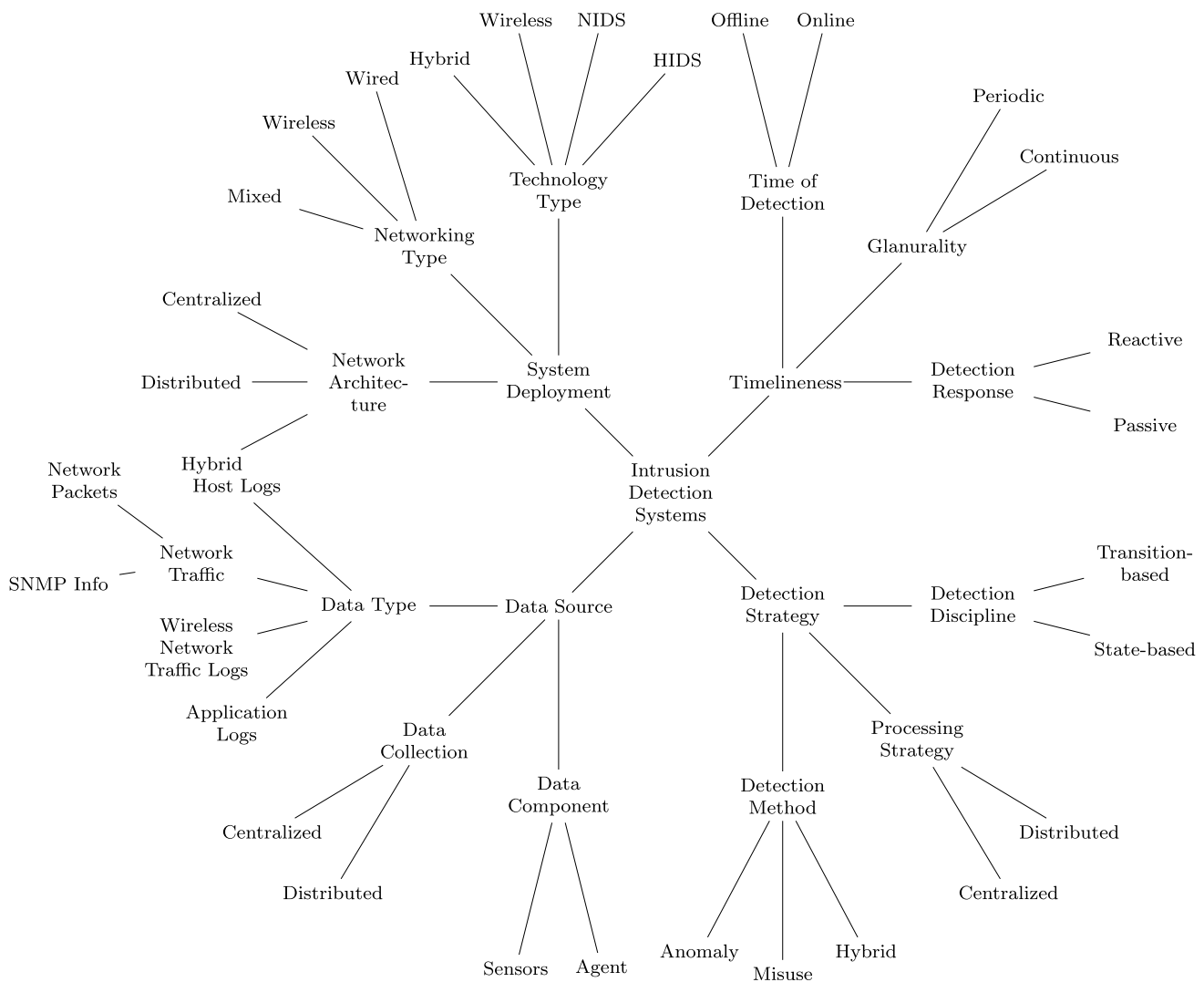


Fig. 2 Taxonomy of intrusion detection system proposed by [21]

in ICSs [30], or particular IDS approach, e.g. anomaly detection [31]. Moreover, most of the survey frameworks are not derived from a systematic review of existing research. Therefore, the coverage and meaningfulness of the frameworks remain insignificant. As far as we can tell, no studies have systematically surveyed the feasibility of utilizing machine learning and deep learning techniques in the purview of intrusion detection in ICSs. Table 2 presents some of the prior applicable reviews and emphasizes the research gaps.

We conduct a systematic mapping study and empirical evaluation focusing on the present literature on intrusion detection in ICSs using machine learning and deep learning techniques to bridge the research gap. A systematic mapping study was initially proposed by [32, 33]. It is a research methodology whose objective is to bring a thorough overview of a field of interest, characterize the research gap, and establish some remarks for future research directions.

Utilizing this procedure, we categorize machine learning and deep learning-based IDSs techniques applied in ICSs, show frequencies of publications, combine the results to answer some detailed research questions, and present a visual summary by mapping the results.

This study fosters the existing literature towards providing state-of-the-art information about implementing machine learning and deep learning techniques for intrusion detection in the industrial control network. We argue that this systematic mapping study will allow researchers or professionals to formulate more proper machine or deep learning-based IDS techniques. Besides, this study is not a cure-all for solving the research challenges in intrusion detection for ICSs; however, this would be a significant outset to develop advancement in employing machine learning and deep learning-based IDS in an industrial control environment.

Table 2 Summary of previous surveys applicable to machine learning and deep learning for intrusion detection in ICSs

Study	Purpose	Constraints	Importance of our study	Research gap
[30]	A taxonomy and a set of metrics for SCADA-specific intrusion detection techniques have been presented	Machine learning and deep learning algorithms have not been discussed	An extensive discussion about machine learning and deep learning for IDS in industrial control network	ML and DL techniques and empirical evaluation were underexplored.
[31]	The authors have provided a roadmap of anomaly detection in industrial networks	IDS techniques, machine learning, and deep learning algorithms have not been included. Specific to anomaly detection machine learning and deep learning algorithms have not been discussed	Both misuse and anomaly detection for industrial networks are discussed	Misuse detection, ML and DL algorithms, and empirical evaluation were underexplored.
[27]	A new taxonomy of IDS for industrial control is provided	The authors have not discussed deep learning	Machine learning and deep learning used for IDS in industrial control network are presented	Machine learning and deep learning techniques
[29]	To provide the use of machine learning on intrusion detection in ICSs	The authors have not discussed deep learning	The use of deep learning is included	Deep learning techniques and empirical evaluation were underexplored.
[28]	The authors summarize previous work for IDSs approaches in industrial control systems	The authors have not discussed deep learning	Discussion on deep learning has been presented	Deep learning techniques and empirical evaluation were underexplored.
[26]	Existing IDS algorithms as well as the software used are studied	The study has not included any deep learning techniques	Deep learning algorithms are primarily included	The usage of deep learning and empirical evaluation were not discussed.

4 Procedure of Mapping Study

This section describes the steps involved in performing a systematic mapping study. It follows the criteria for conducting secondary research proposed by [32] and [34]. Although quality evaluation is required for any systematic review [34], in our mapping study, a quality assessment to filter out main studies is not deemed essential since we structure our analysis to be as broad as feasible. Following the recommendations, we specify the research questions (RQs) being addressed, the search method, and the selection (e.g., inclusion) procedure of primary studies in the following sections.

4.1 Research Questions

As noted by [34], RQs should manifest the objective of secondary studies. RQs also specify the issue to be investigated and direct to the methodology [35]. Hence, the aim and scope of this study are formulated using the following RQs. The first-three RQs would be addressed in Sect. 5, while the rest RQ is covered in Sect. 6.

- (i) RQ_1 : What is the research trend in machine learning and deep learning-based intrusion detection in ICSs?
- (ii) RQ_2 : What types of learning algorithms have been employed to deal with the problems of IDSs in industrial networks?
- (iii) RQ_3 : Which types of intrusion detection techniques are prevalently used in ICSs?
- (iv) RQ_4 : What are the relative performance of AI algorithms for ICS-based IDS?

4.2 Search Method

Despite the fact that machine learning algorithms have been everywhere for more than four decades, however, there exist several issues remain underexplored, leading to a significant increase of interest in utilizing those algorithms to solve real-world problems. As already noted, some elements affecting this flourishing attention for AI are along the following axes: (i) the price of computational resources are depreciating, (ii) the advancement of powerful and efficient algorithms that are able to tackle different forms of data, and (iii) a vast amount of tools that can be employed to facilitate the rapid advancement of AI-based applications.

According to this, we take into account primary studies published over the last six years: from January 2013 to November 2020. We utilized an automatic search to seek as many appropriate primary studies as possible to properly answer the RQs, as mentioned earlier. In particular, we searched two primary digital libraries, i.e., IEEE Digital Library and ACM Digital Library, to incorporate computer-science related journals and conferences. We also searched

the other two well-recognized digital libraries containing computing-related publications, such as SpringerLink and ScienceDirect. To minimize the necessity of searching peculiar sources, two main indexing services, i.e., Web of Science and Scopus, were also taken into consideration. They normally index journals and conferences published in IEEE, ACM, Springer, Elsevier, Taylor & Francis, etc.

To get relevant results while doing a search in such digital libraries, well-defined search terms are required. Thus, keywords were generated from our RQs and from keywords identified in some previously published publications. More precisely, different keyword combinations were tried utilizing Boolean operators, namely AND and OR, resulting in some of the keyword combinations (see Fig. 3).

4.3 Inclusion and Exclusion Criteria

In this section, we specify inclusion and exclusion criteria that were utilized in this study. Obtained papers were filtered in terms of the following criteria, thus only applicable and relevant papers were correctly incorporated. Inclusion criteria are listed as follows.

1. INC_1 : Only publications that were issued in scholarly outlets, i.e. journals, conferences, and workshop proceedings are considered. These papers had been usually refereed by peer-review.
2. INC_2 : Papers that discuss machine learning and deep learning techniques for intrusion detection in industrial control systems were taken into consideration.

Besides, publications that meet at least one of the following criteria were omitted from our study.

1. EXC_1 : The study discusses the application of intrusion detection in ICSs, but machine learning and deep learning are not used. For instance, process mining [36], stateful analysis [37], active monitoring [38], hierarchical monitoring [39], and semantics-aware framework [40].
2. EXC_2 : The studies considered as gray literature, i.e. working papers, presentations, and technical reports.

(Intrusion detection OR anomaly detection OR signature detection OR misuse detection OR attack detection)
AND
(Industrial control network OR Industrial control system OR SCADA OR distributed control system OR PLC OR industrial internet of things OR critical infrastructure)
AND
(Machine learning OR deep learning OR neural network OR ensemble learning)

Fig. 3 Keywords used in the literature search

3. EXC_3 : Non-English publications
4. EXC_4 : Peer-reviewed studies that are not issued in journals, conference and workshop proceedings such as PhD thesis and patents.

5 Mapping Study Result and Discussion

Imbued by the aforementioned RQs, we specify the following magnitudes to outline and examine the selected studies:

- The propensity of research: RQ_1 .
- Publication outlets: RQ_1 .
- Datasets used: RQ_1 .
- Types of machine learning and deep learning algorithms: RQ_2 .
- Types of intrusion detection techniques in ICSs: RQ_3 .

5.1 Mapping Selected Studies w.r.t Year Published

Figure 4 denotes the number of studies over the considered period which is from 2013 to 2020. It is clear that during that period of time, there exist at least one study concerning the use of machine learning and deep learning algorithms for intrusion detection in ICSs environment. According to the trend, there has been a growing interest of applying machine learning and deep learning-based IDS on industrial network. The results indicate that since 2017, there has been a dramatic increase of interest in harnessing ML and DL algorithms for intrusion detection in ICSs.

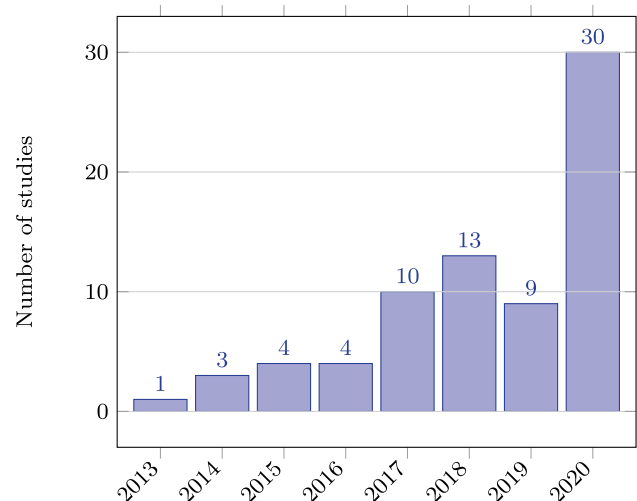


Fig. 4 Distribution of chosen studies during 2013-2020

5.2 Mapping Selected Studies w.r.t. Publication Venue

This section is devoted to summarizing the selected studies (e.g., 74 publications) according to the outlets they appeared. Among the selected studies, the vast majority of studies were disseminated in conference proceedings (e.g., 42 papers), followed by journals (e.g., 26 papers). Figure 5 shows a categorization of the selected studies w.r.t. the publication venue. The selected studies were published as a book section and workshop paper account for five papers and one paper, respectively. Table 3 in Sect. 5.2 breaks down the distribution of selected studies w.r.t. the publication outlets, publication type, number of studies, and the corresponding percentage. The selected studies appeared in 61 different outlets. Two major venues are IEEE Transactions on Industrial Informatics and Chinese Control and Decision Conference that published three papers each. Other notable venues are IEEE International Conference on Computer and Communications; International Conference on Availability, Reliability, and Security; IEEE Internet of Things Journal; IEEE Access; International Journal of Critical Infrastructure Protection; Applied Soft Computing; Neural Computing and Applications; International Joint Conference on Neural Networks; and Inventive Communication and Computational Technologies.

5.3 Mapping Selected Studies w.r.t Dataset Considered

This section outlines the selected studies concerning the datasets considered in the experiment. Nowadays, there is a growing need to utilize multiple datasets for validating the proposed detection model. It is required to prove the generalizability of the model in different ICS environment

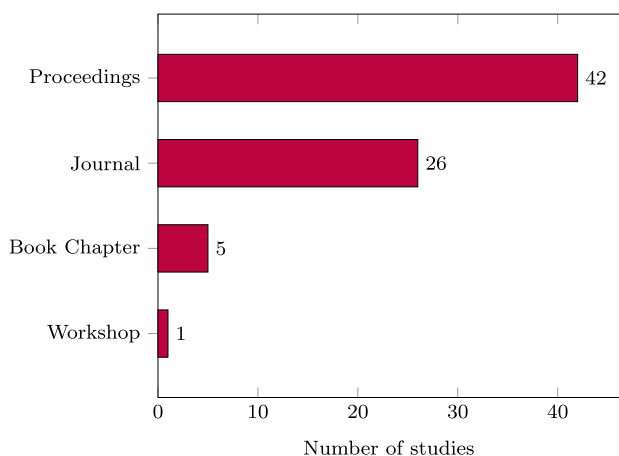


Fig. 5 Distribution of selected studies w.r.t publication venues

settings. However, as indicated in Tables 6, 7, 8 and 9, in most cases, researchers only considered one single dataset in their experiment. Therefore, it can be assumed that the major flaw of the selected studies is the model's generalizability. Table 4 depicts the number of IDS datasets in the current literature. It is worth mentioning that most datasets (e.g., used in 29 papers) are not publicly available (e.g., private); thus, it would not be easy to make the experiment reproducible and comparable. Several studies (e.g., [41–47]) even used inappropriate datasets (e.g., NSL-KDD, KDD Cup 99, and DARPA 1998) which are not specifically applicable in ICS environment. Other prominent datasets for IDS in industrial control network are gas pipeline and power system that appeared eighteen and eleven times in the literature, respectively.

5.4 Mapping Selected Studies w.r.t. Algorithms

There is a large number of ML algorithms that are commonly categorized into two learning approaches, i.e., supervised and unsupervised. A supervised learner deals with a process of learning from the labeled training data that can be represented as follows.

$$D = \{(x_1, y_1), \dots, (x_n, y_n) : n \in \mathbb{N}\} \quad (1)$$

where $x_i \in \mathcal{X}$ are m -dimensional feature input vectors ($m \in \mathbb{N}$) and $y_i \in \mathcal{Y}$ are the corresponding output variable, e.g. target value. Labeled training data are employed to fit a predictive model that assigns labels on new samples given label training data. Roughly speaking, a model is used to learn the mapping function identified in the training data: $\mathcal{X} \rightarrow \mathcal{Y}$ [115]. On the contrary, unsupervised learning deals with discovering the fundamental relationship between the inputs, where the objective is to assign the inputs into different groups [116]. Clustering is an example of unsupervised learning algorithms. However, some algorithms are not suitable for being grouped into supervised or unsupervised. These such algorithms are regarded as semi-supervised learning that deals with the learning tasks by employing both labeled and unlabeled datasets. According to the results of our mapping study, most intrusion detection approaches in ICSs are addressed and handled as supervised learning (see Table 5). There exist only, respectively, eight and two studies that resolved unsupervised and semi supervised learning for intrusion detection in ICSs. In addition, there has been a great *hype* on the use of deep neural network algorithms, e.g. recurrent neural network (RNN), convolutional neural network (CNN), and autoencoder.

Table 3 Summarization of the outlets where the selected studies were published in

No	Publication outlet	Type	Number of studies	%
1.	International Conference on Machine Learning and Applications	Conference	1	1.35
2.	International Conference on High Confidence Networked Systems	Conference	1	1.35
3.	IEEE Transactions on Industrial Informatics	Journal	3	4.05
4.	Computers & Security	Journal	1	1.35
5.	Annual IEEE India Conference	Conference	1	1.35
6.	IEEE Transactions on Dependable and Secure Computing	Journal	1	1.35
7.	World Congress on Industrial Control Systems Security	Conference	1	1.35
8.	Journal of Process Control	Journal	1	1.35
9.	Information Security Research and Education Conference	Conference	1	1.35
10.	IFIP International Conference on Information Security Theory and Practice	Conference	1	1.35
11.	International Conference on Computational Science and Computational Intelligence	Conference	1	1.35
12.	International Conference on Software Security and Assurance	Conference	1	1.35
13.	International Conference on Soft Computing, Intelligent System and Information Technology	Conference	1	1.35
14.	IEEE International Conference on Big Data	Conference	1	1.35
15.	IEEE European Symposium on Security and Privacy Workshops	Conference	1	1.35
16.	IEEE International Conference on Emerging Technologies and Factory Automation	Conference	1	1.35
17.	Chinese Control And Decision Conference	Conference	3	4.05
18.	IEEE International Conference on Computer and Communications	Conference	2	2.70
19.	International Conference on Availability, Reliability, and Security	Conference	2	2.70
20.	International Journal of Computer Theory and Engineering	Journal	1	1.35
21.	IEEE Annual International Conference on Cyber Technology in Automation, Control, and Intelligent Systems	Conference	1	1.35
22.	International Conference on Engineering Applications of Neural Networks	Conference	1	1.35
23.	Science, Engineering & Education	Journal	1	1.35
24.	IEEE International Conference on Intelligence and Security Informatics	Conference	1	1.35
25.	IEEE International Conference On Trust, Security And Privacy In Computing And Communications/IEEE International Conference On Big Data Science And Engineering	Conference	1	1.35
26.	IEEE International Conference on Cloud Computing and Big Data Analysis	Conference	1	1.35
27.	Workshop on Cyber-Physical Systems Security and Privacy	Workshop	1	1.35
28.	Journal of Parallel and Distributed Computing	Journal	1	1.35
29.	IEEE International Performance Computing and Communications Conference	Conference	1	1.35
30.	IEEE Global Communications Conference	Conference	1	1.35
31.	IEEE International Conference on Industrial Informatics	Conference	1	1.35
32.	International Conference on Applied Computing and Information Technology	Conference	1	1.35
33.	Future Internet	Journal	1	1.35
34.	IEEE Internet of Things Journal	Journal	2	2.70
35.	IEEE International Conference on Communications	Conference	1	1.35
36.	International Symposium for ICS & SCADA Cyber Security Research	Conference	1	1.35
37.	Sensors	Journal	1	1.35
38.	IEEE Conference on Communications and Network Security	Conference	1	1.35
39.	Intelligent Systems Applications in Software Engineering	Book Chapter	1	1.35
40.	International Conference on Industrial Engineering, Applications and Manufacturing	Conference	1	1.35
41.	IEEE International Conference on Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing, and IEEE International Conference on Intelligent Data and Security	Conference	1	1.35
42.	International Conference on Software, Telecommunications and Computer Networks	Conference	1	1.35
43.	IEEE Transactions on Network and Service Management	Journal	1	1.35
44.	Journal of Ambient Intelligence and Humanized Computing	Journal	1	1.35
45.	Renewable Energy	Journal	1	1.35
46.	IEEE Access	Journal	2	2.70

Table 3 (continued)

No	Publication outlet	Type	Number of studies	%
47.	IEEE Transactions on Industry Applications	Journal	1	1.35
48.	International Journal of Critical Infrastructure Protection	Journal	2	2.70
49.	Applied Soft Computing	Journal	2	2.70
50.	Neural computing and applications	Journal	2	2.70
51.	Energy Informatics	Journal	1	1.35
52.	Computers & Security	Journal	1	1.35
53.	International Joint Conference on Neural Networks	Conference	2	2.70
54.	Conference on Innovation in Clouds, Internet and Networks and Workshops	Conference	1	1.35
55.	ACM Southeast Conference	Conference	1	1.35
56.	International Conference on Dependable Systems and Their Applications	Conference	1	1.35
57.	IEEE-HYDCON	Conference	1	1.35
58.	IEEE Conference on Control Technology and Applications	Conference	1	1.35
59.	Design and Analysis of Distributed Energy Management Systems	Book Chapter	1	1.35
60.	Inventive Communication and Computational Technologies	Book Chapter	2	2.70
61.	Security of cyber-physical systems	Book Chapter	1	1.35

Table 4 Recapitulation of chosen studies based on the datasets utilized

Dataset	Selected studies	Number of studies
Gas pipeline	[44, 48–64]	18
Water storage	[44, 49, 50, 53, 55, 59, 62, 65]	8
Power system	[53, 62, 66–74]	11
SWaT	[64, 75–81]	8
NSL-KDD	[41–43]	3
DARPA 1998	[44, 46]	2
KDD Cup 99	[45, 47]	2
Private	[47, 65, 82–108]	29
Others	MAXI [109], Electric Transmission [50], Vx Heaven [110], GPNS [111], SCADA Network [112], CICIDS 2017 [113], BATADAL [114]	7

5.4.1 Supervised Learning

Work in [97] studied the most prevalent vulnerabilities in SCADA IIoT and used ML-based algorithms to combat them. Seven different classifiers were tested for IDS such as support vector machine (SVM), *K*-nearest neighbor (KNN), naive Bayes (NB), random forest (RF), decision tree (DT), logistic regression (LR), and artificial neural network (ANN). The experimental results indicate that RF shows the best performance, and LR has the worst performance in terms of ROC curve. Similarly, Teixeira et al. [96] used several ML algorithms, i.e., LR, RF, NB, SVM, and KNN to detect cybersecurity attacks in a SCADA system by developing a testbed environment. An SVM-based cooperative

training model (SCTM) is proposed in [98] to improve the effectiveness of detecting ICSs attacks. Anton et al. [57] compared SVM and RF for anomaly-based intrusion detection in an industrial network, in which RF slightly outperformed SVM in terms of accuracy metric.

Besides, DT and Bayesian network classifiers were compared for anomaly-based intrusion detection in SCADA network [51]. Terai et al. [87] incorporated SVM to construct a discriminant model between normal and anomalous packets based on the ICSs communication profile. Considering the same ML algorithm, e.g., SVM, Li et al. [52] had attempted to optimize SVM's learning parameters using a velocity adaptive shuffled frog leaping bat algorithm for ICSs intrusion detection. Li and Qin [88] applied five different ML

Table 5 Artificial intelligence techniques for ICS-based IDS are categorized into several algorithm families

Learning task	Algorithm's family	Studies	Total
Supervised	Tree-based	Decision tree [44, 45, 51, 58, 61, 64, 82, 85, 88, 90, 91, 97, 103, 106]	14
		Fuzzy-based decision tree [66, 83]	2
		REPT [82]	1
		Decision stump [82]	1
		Random tree [63]	1
		Hoeffding tree [63]	1
	Ensemble-based	Random forest [45, 48, 54, 57, 67–69, 88, 96, 97, 106, 107]	12
		Gradient boosting [88, 106]	2
		Bagging [68, 82, 106]	3
		Dagging [82]	1
		Adaboost [45, 68, 90, 106]	4
		Random subspace [71, 100]	2
		Majority voting [67, 68, 114]	3
		Stacking [47]	1
	Generalized linear-based	Support vector machine [41, 43, 44, 48, 49, 52, 54, 57, 58, 67, 70, 87, 88, 90, 91, 96–99, 103, 106–108]	23
		Linear discriminant analysis [90]	1
		Logistic regression [41, 82, 91, 96, 97]	5
	Instance-based	K-nearest neighbor [48, 58, 61, 67, 73, 86, 88, 90, 91, 96, 97, 100, 103, 106]	14
		Principle component analysis [49]	1
	Rule-based	Ridor [82]	1
		OneR [48, 63]	2
		Logical analysis [81]	1
	Probabilistic-based	Naive Bayes [45, 48, 63, 70, 82, 89, 96, 97, 103, 106]	10
		Naive Bayes multinomial [82]	1
		Hidden Markov model [50]	1
		Bayesian network [51, 63]	2
	Neural-based	Neural network [53, 70, 72, 78, 92, 97, 113]	7
		Convolutional neural network [75, 76, 80, 93, 101]	5
		Recurrent neural network [75, 77, 112], LSTM and GRU [56], LSTM [111]	6
		Deep belief network [41, 110]	2
		Deep neural network [42, 102]	2
		Generative adversarial network [59]	1
Unsupervised	Clustering	K-means [46, 58, 66]	3
		Local outlier factor [44]	1
		Isolation forest [74, 80, 94]	3
	Generalized linear-based	One-class support vector machine [44, 94]	2
	Neural-based	Autoencoder [41, 64, 79, 95, 103–105, 113]	8
		Restricted Boltzman machine [107]	1
		Self-organizing maps [109]	1
	Association rules-based	FP-growth [45]	1
		Apriori [84]	1
Semi-supervised	Clustering	K-means [55, 65]	2
	Generalized linear-based	One-class support vector machine [55, 108]	2
	Neural-based	Spiking neural network [62]	1
		Autoencoder [60]	1

Table 6 Summarization of primary studies by detection technique, domain of interest, and other relevant categories in chronologically order from 2013 to 2016

Author(s)	Type	Tasks	Dataset	Performance metric	Remark
Beaver et al. [48]	Hybrid	Classification	Gas pipeline	Precision and recall	Best-performing algorithm was not mentioned
Mantere et al. [109]	Anomaly	Features specification	MAXI	Not mentioned	Performance evaluation is further needed
Nader et al. [49]	Anomaly	Classification	Gas pipeline and water storage [48, 118]	Detection rate	Kernel selection
Almalawi et al. [65]	Anomaly	Classification	Two private datasets and water storage [118]	Detection rate, false positive, Precision, and F_1	High computational overhead
Samdarshi et al. [45]	Misuse	Classification	KDD Cup 99	Accuracy	An IDS dataset for conventional IT was used
Ponomarev and Atkison [82]	Anomaly	Classification	Private	Accuracy	Variety of attacks were not covered
Hosic et al. [83]	Anomaly	Classification	Private	Accuracy	More rich feature set is necessary
Khalili and Sami [84]	Anomaly	Rule generation	Private	Not mentioned	Involving expert's opinion
Tomlin et al. [66]	Misuse	Cluster analysis and classification	Power system [119]	True positive, false positive, and true negative	Validated on a single dataset
Stefanidis and Voyiatzis [50]	Misuse	Classification	Gas pipeline, water tower, and electric transmission [48, 118, 120]	Detection rate	Number of hidden states can affect the system efficiency
Ponomarev and Atkison [85]	Anomaly	Classification	Private	Accuracy	Limited number of features were considered
Eigner et al. [86]	Misuse	Classification	Private	Not mentioned	Detected only a particular attack

techniques, i.e., KNN, RF, DT, SVM, and gradient boosting for malicious identification in ICSs. From the experimental result, it revealed that DT achieved the highest accuracy, followed by RF. A naive Bayes (NB) classifier was also employed by [89] for attack detection in cyber-physical systems (CPSs), which are usually controlled and monitored by an ICSs.

Francia [90] proposed test datasets using an ICSs tested and employed machine learning algorithms, i.e., AdaBoost, complex DT, KNN, SVM, and linear discriminant model for evaluating the generated test dataset. A one-class anomaly detection framework based on neural network was studied in [53]. The proposed classifier was trained exclusively with normal traffic data of ICSs, yet it was able to detect abnormalities involved with advance persistent threat (APT) attacks. Stefanidis and Voyiatzis [50] presented a new approach of intrusion detection in ICSs environment using a hidden Markov model (HMM). The proposed method is more suitable for real-time applications since it produces the results on a per-packet basis. A decision tree classifier combined with session duration-based feature extraction for intrusion detection in a control system network is suggested by [85].

Detection of a particular attack, i.e., man-in-the-middle in industrial control network had been discussed [86]. A machine learning algorithm, i.e., KNN with Bregman divergence was proposed to specify normal behavior. Samdarshi et al. [45] discussed a number of ML algorithms, i.e., DT, RF, NB, and AdaBoost for SCADA security. The proposed IDS technique was built based on a three-layer detection system. By analyzing the ICSs network's telemetry data, Ponomarev and Atkison [82] classified the network traffic data using several ML algorithms, i.e. bagging, dagging, decision stump, LR, REPT, DT, NB, NB multinomial, and Ridor. A fuzzy logic-based decision tree to detect anomalies in ICSs networks was exploited in [83]. The proposed method evolved a combination of DT and genetic programming. A one-class classification, e.g., having only samples from a particular class of training dataset for detecting intrusions on industrial systems is presented in [49]. Two different approaches were studied: support vector data description (SVDD) and kernel principal component analysis (KPCA).

Subsequently, different kinds of machine learning algorithms, i.e., KNN, SVM, LR, and DT, were employed to detect DCS's abnormal traffic. Several effective features were obtained using a dual window scheme [91]. In the same vein, Beaver et al. [48] benchmarked several ML techniques, i.e., NB,

Table 7 Summarization of primary studies by detection technique, domain of interest, and other relevant categories in 2017

Author(s)	Type	Tasks	Dataset	Performance metric	Remark
Vávra and Hromada [67]	Anomaly	Classification	Power system [119]	True positive rate, false positive rate, positive predictive value, and F_1	The performance of the predictive model was not satisfying on multiclass datasets
Ullah and Mahmoud [51]	Hybrid	Classification	Gas pipeline [48, 120]	Precision, recall, and F_1	More types of attacks are needed
Teraï et al. [87]	Anomaly	Classification	Private	Precision, recall, F_1 , and Error rate	SVM mode had many parameters
Potluri et al. [41]	Misuse	Classification	NSL-KDD [121]	Precision, recall, and F_1	Use conventional IDS dataset
Li et al. [52]	Misuse	Classification	Gas pipeline [48, 120]	Detection rate, false positive rate, and false negative rate	Parameter optimization of SVM is necessary
Li and Qin [88]	Anomaly	Classification	Private	Accuracy	Limited number of training samples
Kreimel et al. [89]	Misuse	Classification	Private	Not mentioned	Other attacks, i.e. replay and passive attacked were not covered
Potluri and Diedrich [42]	Misuse	Classification	NSL-KDD [121]	Precision, recall, and F_1	Use conventional IDS dataset
Francia [90]	Anomaly	Classification	Private	Accuracy, Precision, Recall, Specificity, and Informedness	Granularity of the dataset needs to be improved
Demertzis et al. [53]	Anomaly	Classification	Power system, gas pipeline, and water storage [48, 118–120]	Precision, recall, F_1 , and AUC	Further optimization of the algorithm parameters are needed

RF, OneR, KNN, and SVM, for identifying malicious activities on SCADA communications. Smith et al. [99] utilized a one-class SVM to detect anomalous/unwanted activity during ICSs maintenance by observing the network traffic for factory interface network service (FINS) devices. A combination of random subspace learning and K-nearest neighbor to defend against the forged commands which target the industrial control process was studied in [100]. Zong et al. [43] adopted an SVM classifier for intrusion detection based on traffic research in industrial control systems. Furthermore, the imbalanced data problem in anomaly detection for IIoT was studied in [92]. The paper investigated the efficiency of artificial neural networks in detecting anomalies through different imbalance ratios.

An evaluation of two machine learning algorithms, i.e., SVM and RF, for intrusion detection in the SCADA system was conducted in [54]. The experimental result revealed that RF detected intrusion effectively in terms of F_1 score > 99%. Unlike ordinary individual classifiers, classifier ensembles train multiple classifiers and combine them for prediction [117]. It is common knowledge that a classifier ensemble is generally significantly more accurate than individual classifiers. This motivated [68] to explore the suitability of classifier ensembles as an apparatus of detecting power system cyber-attacks. The proposed detection model relied on several different ensemble schemes, i.e., adaptive boosting, bagging, majority voting, and RF. In addition, Vávra and Hromada [67] utilized majority voting to combine three ML

algorithms, i.e., IB1, RF, and SVM, to evaluate the predictive model for intrusion detection on ICSs.

As mentioned, deep learning algorithms have received tremendous interest in the intrusion detection field. Kravchik and Shabtai [75] studied 1D convolutional neural network (CNN) for detecting cyber-attacks on ICSs. A variety of deep neural architectures, including different variants of convolutional and recurrent networks, were applied. Furthermore, a deep belief network (DBN) based threat detection model for the SCADA system was investigated in [110]. The proposed model provided an adaptive mechanism to the dynamic changes in new malware variants. Yang et al. [101] proposed deep learning-based intrusion detection for SCADA systems. The proposed method utilized CNN to define a salient temporal pattern of SCADA traffic and identify the time windows in which attacks exist. Furthermore, rather than proposing an anomaly-based intrusion detection, Potluri and Diedrich [42] used a deep neural network (DNN) to identify the different types of attacks in IDS.

Using a similar method, Liu et al. [93] proposed a two-level anomaly detector framework. In the first level, CNN was used to feature extraction and anomaly identification, while a process state transfer algorithm was taken into consideration in the second level. Vávra and Hromada [112] introduced a genetic algorithm to optimize a recurrent neural network for industrial network anomaly detection. Two different recurrent neural network architectures, i.e., LSTM

and gated recurrent unit (GRU), were proposed for intrusion detection on the Gas pipeline dataset [56]. Similarly, Yang et al. [111] proposed a stealthy attack detection in ICSs using multi-dimensional data fusion, while LSTM was deployed to model the normal behavior of ICSs. Work in [41] evaluated the performance of the detection mechanism by combining DL and ML techniques. Two ML algorithms, i.e., softmax regression and SVM, and two deep learning algorithms, i.e., stack autoencoder and DBN, were used in the benchmark.

Upadhyay et al. [69] focused on selecting the most promising features using gradient boosting feature selector. Süzen [102] found that DBN was a preferred method for detecting malicious attacks in network traffic. Hidden layers were updated using contrastive divergence, while the output layer is combined with a softmax classifier. Robles-Durazno et al. [103] used energy-based features and compared five traditional machine learning algorithms for real-time anomaly detection in a water supply system. Ramotsoela et al. [114] proposed a voting-based ensemble technique to enhance a behavioral-based IDS in the water distribution system. Priyanga et al. [76] presented a hypergraph-based anomaly detection with enhanced PCA and CNN. Phillips et al. [58] evaluated the viability of ML techniques in detecting new security threats specific to the SCADA system. Likewise, Onoda [44] compared supervised and unsupervised-based IDS methods. He concluded that supervised methods could achieve the same performance as unsupervised ones if we have sufficient training samples.

Neha et al. [77] presented a sine-cosine optimization-based RNN to detect the cyber-physical attacks against SCADA systems. MR et al. [78] proposed a multi-layer perceptron model for anomaly detection in ICSs. A cumulative sum is integrated with MLP to detect abnormal deviations in the sensor values due to attacks. Mozaffari et al. [70] presented a comparison of supervised ML methods for classifying power system behaviors and detecting future attacks. Liu et al. [59] proposed a bidirectional generative adversarial network in ICS intrusion detection. The proposed method showed better accuracy and shorter detection time than other baselines. Lan et al. [106] benchmarked several ML methods for classifying network traffic data in ICS to detect man-in-the-middle attack. Hassan et al. [71] improved the trustworthiness of an IIoT network through a scalable and reliable cyberattack detection model. Specifically, a random subspace ensemble model with a random tree classifier was employed to overcome the overfitting problem.

Hallaji et al. [61] employed several feature selection techniques, called multi-subspace feature selection to perform intrusion detection in smaller subspace, which brought about efficiency and accuracy. Haghnegahdar and Wang [72] applied a whale optimization algorithm to initialize and adjust the ANN's weight vector to achieve the minimum mean square error. The proposed model could address the challenges of attacks, failure prediction, and failure detection in a power system. Gumaei

et al. [73] considered CFS-based feature selection to remove irrelevant features, while KNN was used to classify normal and cyberattack events. Gao et al. [47] proposed a stacking ensemble to fuse LSTM and feedforward neural network. Combining LSTM and neural network through an ensemble approach further improves the IDS performance with F_1 of 99.68% regardless of the data packets' temporal correlations.

Egger et al. [108] benchmarked various ML techniques for addressing security concerns in the ICS domain. Specifically, both supervised and unsupervised learning methods were assessed for intrusion detection in substations, which use the asynchronous communication protocol International Electrotechnical Commission (IEC) 60870-5-104. Das et al. [81] designed a rule-based system to detect any change in sensor measurements' behaviors due to an attack. The rules were extracted from historical sensor measurements, and these rules can categorize the condition of a plant. Choubineh et al. [63] considered the techniques of cost-sensitive learning and Fisher's (e.g., linear) discriminant analysis (FDA) to overcome class imbalance issues in SCADA system datasets using five different ML algorithms.

5.4.2 Unsupervised Learning

A new approach to detect malicious activities in the ICSs network using a clustering technique was considered in [46]. In order to detect abnormal patterns, a simple K-means algorithm was employed. Schuster et al. [94] discussed two popular unsupervised learning methods, i.e., one-class SVM and isolation forest, to build a self-adaptive anomaly detector. On top of that, another variant of deep learning that works in unsupervised mode, e.g., autoencoder had been introduced in [41, 64, 79, 95, 103–105, 113]. Using autoencoder, the proposed model could detect replay attack's abnormal traffic by learning the inter-packet arrival time. Moreover, a classical frequent itemset mining algorithm, e.g., FP-Growth, was taken into account in [45]. Another frequent itemset mining, e.g., Apriori for state-based IDS in an industrial network, was suggested by [84].

Similarly, autoencoder and DBN were used in [41] for feature extraction in order to achieve the best performance of intrusion detection in network control systems. An unsupervised anomaly-based IDS based on clustering technique was proposed in [66]. The clustering approach was made up of four main processes, i.e., data preprocessing, cluster analysis, features generation from cluster, and states classification using a fuzzy inference system. Furthermore, Mantere et al. [109] used self-organizing maps (SOMs) for anomaly detection in ICSs networks. Hassan et al. [107] used restricted Boltzman machine to extract the features from unlabeled data, while SVM and RF were used to detect the unlabeled attacks. Elnour et al. [80] combined isolation forest and CNN as a hybrid attack detection approach for ICSs. The proposed approach was applied to the SWaT testbed and showed an improvement

over the other works in terms of detection capability. Chaithanya et al. [74] proposed an outlier detection approach using salp swarm optimization-based isolation forest. The proposed model was used to build an efficient SCADA intrusion detection system and tested it on the power system dataset.

5.4.3 Semi-supervised Learning

A study in [55] discussed semi-supervised learning to generate large scale training datasets using few labeled data samples using the K-means algorithm and one-class SVM. Almalawi et al. [65] proposed KNN and fixed-width clustering technique for detecting cyber-attacks. The proposed techniques provide considerable accuracy compared to well-known anomaly detection techniques. Joshi et al. [60] used autoencoder in a semi-supervised way to detect malicious behavior in SCADA used to control gas pipeline system. Demertzis et al. [62] developed and tested an anomaly detection algorithm, called Gryphon. It is a semi-supervised unary anomaly detection system evolving spiking neural network one-class classifier.

5.5 Mapping Selected Studies w.r.t. IDS Approaches

Following an IDS taxonomy presented in [21], we classify the primary studies based on three primary IDS detection techniques, i.e., anomaly, misuse, and hybrid-based approaches (see Fig. 6). The greatest number of selected studies have taken into account the anomaly-based approach (about 67.57%), while misuse and hybrid-based approach share about 17.57% and 14.86% of the total selected studies, respectively. Besides, we also categorize the primary studies based on the area of concern. Tables 6, 7, 8 and 9 summarize 74 studies that propose intrusion detection for ICSs based on machine learning and deep learning techniques. These tables also show for each study the following information: (i) machine learning and deep learning task, (ii) the considered datasets, (iii) the utilized performance metrics, and (iv) remarks for the further research problem.

6 Empirical Study

Empirical evaluation is the most often used technique for assessing the performance of algorithms. This research extends the scope of the previous article by giving an empirical benchmark for numerous machine learning and deep learning methods used for IDS in industrial control networks. This section compares the performance of the algorithms used to address *RQ4*.

6.1 Classification Methods

This benchmark includes five classification algorithms, i.e., random forest (RF), gradient boosting machine (GBM),

XGBoost, and deep neural network (DNN) implemented in *R*. The classifiers were chosen since they have relatively received little attention in the current literature. Note that, currently available works involving ensemble learning for IDS in ICS, such as [126] and [127], respectively, use individual XGBoost and majority voting approaches. Hence, to justify the contribution of this empirical study, a stacked generalization [128, 129] technique is proposed since it has not been previously taken into account in the literature (Table 10).

The stacking combines several base learners, i.e., RF, GBM, XGBoost, and DNN altogether, hence enhancing the diversity of ensemble. Besides, a GBM is employed as a meta-classifier to get the final prediction. The procedures used to construct the stacked generalization ensemble considered in the experiment are as follows: (i) we train and validate each base classifier $\mathcal{B}$ using ten-fold cross-validation on the training set and collect the prediction results $\mathcal{R}$; (ii) each base classifier's prediction result is combined in such a way that a new matrix $\mathcal{G}$ is created. Train the meta-classifier on the level-1 data in conjunction with the response vector; and (iii) to obtained the final prediction, stacked generalization model and meta model are used to validate the testing set. To conclude, Algorithm 1 describes the complete process of constructing the stacked generalization ensemble.

Algorithm 1: Stacked generalization ensemble with internal cross-validation for attack detection in ICS.

Input:

ICS dataset, $\mathcal{D}$ with v instances and w features, which is denoted as input matrix $\mathcal{X}$ and response matrix $\mathcal{Y}$; training set, $\mathcal{D}_{train}$; testing set, $\mathcal{D}_{test}$; $\mathcal{B}$ base classifiers; and meta classifier, $\mathcal{M}_c$.

Output: Final ensemble prediction, $\mathcal{F}_e$.

Begin

1. Build the classification model:

1.1. Train $\mathcal{B}$ base classifiers on $\mathcal{D}_{train}$

1.2. Apply *stratified* 10-fold cross-validation on each $\mathcal{B}$ base classifier.

1.3. Take the prediction results, $\mathcal{R}_1, \mathcal{R}_2, \dots, \mathcal{R}_{\mathcal{B}}$

1.4. Take $\mathcal{T}$ prediction values from $\mathcal{B}$ base classifiers and construct a matrix $\mathcal{T} \times \mathcal{B}$, which is later called as matrix $\mathcal{G}$.

1.5. Along with original response vector $\mathcal{Y}$, train $\mathcal{M}_c$: $\mathcal{Y} = f(\mathcal{G})$.

$$v \left\{ \begin{bmatrix} \mathcal{R}_1 \end{bmatrix} \dots \begin{bmatrix} \mathcal{R}_{\mathcal{B}} \end{bmatrix} \begin{bmatrix} \mathcal{Y} \end{bmatrix} \right\} \rightarrow \mathcal{T} \left\{ \overbrace{\begin{bmatrix} \mathcal{G} \end{bmatrix}}^{\mathcal{B}} \begin{bmatrix} \mathcal{Y} \end{bmatrix} \right\}$$

2. Make a prediction:

2.1. Use the classification model on $\mathcal{D}_{test}$.

2.2. Acquire the prediction results from each $\mathcal{B}$ base classifier and feed into $\mathcal{M}_c$.

2.3. Acquire $\mathcal{F}_e$.

End

Table 8 Summarization of primary studies by detection technique, domain of interest, and other relevant categories in 2018

Author(s)	Type	Tasks	Dataset	Performance metric	Remark
He et al. [91]	Hybrid	Feature extraction and Classification	Private	Accuracy and AUC	Near-perfect detection rate is still questionable
Zong et al. [43]	Anomaly	Classification	NSL-KDD [121]	Accuracy, detection rate, and false alarm rate	More types of attack features are needed to be addressed
Zolanvari et al. [92]	Anomaly	Classification on imbalanced dataset	Private	Accuracy, false alarm rate, undetected rate, sensitivity, and Matthews correlation coefficient	Only one classifier was used
Perez et al. [54]	Hybrid	Classification	Gas pipeline [48, 120]	Accuracy, precision, recall, and F_1	Used only limited number of classifiers
Chen et al. [68]	Anomaly	Classification	Power system [119]	Accuracy, precision, recall, and F_1	Tested on a wider classification schemes is necessary
Kravchik and Shabtai [75]	Anomaly	Classification	SWaT [122]	F_1 and AUC	Timeliness of the attack detection is further needed to be investigated
Huda et al. [110]	Anomaly	Classification	Vx Heaven [123]	Accuracy, false positive rate, and false negative rate	Lacked of GPU and parallel computation
Liu et al. [93]	Anomaly	Classification	Private	Accuracy, precision, recall, and F_1	Features extracted by CNN was less interpretable
Yang et al. [111]	Anomaly	Classification	GPNS	AUC	Proposed classifier was validated on single dataset
Schuster et al. [94]	Anomaly	Cluster analysis and classification	Private	Precision, recall, and F_1	Some attacks were not addressed
Hong et al. [95]	Anomaly	Cluster analysis	Private	Not mentioned	Utilized small attack samples
Yang and Zhou [55]	Anomaly	Training data generation using few samples and classification	Gas pipeline and water storage [48, 118, 120]	Accuracy, detection rate, and false positive rate	Hybrid kernel function is further needed to be addressed
Teixeira et al. [96]	Anomaly	Classification	Private	Accuracy and false positive rate	Generating more attacks is required

The experiment makes use of a machine learning framework named *H2O* [130] that offers an interface in *R*. All parameters were determined using the *random search* [131] command. The base classifiers used in this work, together with their optimum hyperparameters, are briefly described below.

(a) *Random forest* (RF) [132]. It has been intensively employed due to its ability in reducing the overfitting while improving the classification accuracy. It grows many classification trees in the forest. Each tree provides a vote for the class, and the forest's final prediction is made using the most votes. The forest error rate relies on the correlation between any trees in the forest and each tree's strength in the forest. Many trees (e.g., 500) are used to build the forest, while other learning parameters are set as follows. Maximum depth = 2, nbins = 1024, nbins cats = 64, sample rate = 0.56, col

sample rate change per level = 1.04, and col sample rate per tree = 0.62.

(b) *Gradient boosting machine* (GBM) [133]. The principle of boosting lies in the idea of whether a weak classification algorithm can be converted to become a strong classifier. GBM involves several elements to work. Those are a loss function is to be optimized, a weak classifier to make predictions, and an additive model, i.e., gradient descent procedure, to add a weak classifier to minimize the loss function. Decision trees are used as a weak classifier in gradient boosting. In the experiment, we employed 500 decision trees, maximum depth = 19, minimum rows = 2, nbins = 1024, nbins cats = 64, learn rate = 0.05, col sample rate change per level = 1.1, learn rate annealing = 0.99, col sample rate = 0.80, and col sample rate per tree = 0.80.

(c) *Extreme gradient boosting machine* (XGB) [134]. It has been dominating applied ML benchmarks for tabular

data, and an implementation of gradient boosted decision trees focusing on computational speed and model performance. XGBoost follows the same principle as GBM; however, it uses a more regularized model to control overfitting. Optimal parameters are set as follows. Number of trees = 500, maximum depth = 8, min rows = 5, learn rate = 0.05, sample rate = 0.42, col sample rate = 0.80, and col sample rate per tree = 0.39. A faster implementation of XGBoost using GPU-based computation is also enabled.

- (d) *Deep neural network* (DNN) [14]. It is derived from a multilayer feed forward neural network that is constructed using stochastic gradient descent of back-propagation. When it comes to DNN models, feedforward artificial neural networks (ANNs) or multilayer perceptron are the most prevalent and the only ones supported natively in *H2O*. The number of hidden layer is set to 3, where the number of neurons is 258, 516, and 258 for the first, second, and third hidden layer, respectively. Other learning parameters are set as follows. Activation function is rectifier with dropout, epochs = 1000, $l_1 = 0.00001$, $l_2 = 0.0001$, rate = 0.05, $\rho = 0.99$, $\epsilon = 1 \times 10^{-8}$, and adaptive rate is disabled (Table 11).

6.2 Materials

This section discusses the datasets that are prevalently considered for ICS and IIoT cyber-attack detection. We briefly outline the datasets as follows. We excluded several datasets, including Gas Pipeline, Water Storage Tank [135], and New Gas Pipeline [120] due to flaws and criticisms such as machine learning's misclassification error, the ease with which machine learning algorithms can achieve 100 percent accuracy, and missing values in the data. The characteristics of each dataset is summarized in Table 12, which also includes a calculation of the imbalance ratio, despite the fact that the majority of datasets are imbalanced. The imbalance ratio is defined as a ratio of the number of samples from the majority class (i.e., natural class) to the number of samples from the minority class (i.e., attack class). In the other words, the higher ratio means a less skewed dataset.

- (a) *Power systems* [136]. The power system datasets¹ is comprised of fifteen sets, namely P1, P2, ..., P15, where the number of input features in each set is 128 and one target feature. Each dataset includes the measurements related to electric transmission normal, disturbance, control, and cyber-attack behavior. One hundred six-

teen features were obtained from 29 types of measurements from each phasor measurement unit (PMU), while 12 features were obtained from control panel logs, Snort alert, and relay logs. There is a total of 37 power system event scenarios, which can be classified as natural events (8), no events (1), and attack events (28) (see Table 11). The target feature consists of a binary marker that indicates attack and natural traffic.

- (b) *WUSTL-IIoT-2018* [137]. The dataset² was developed using the SCADA system testbed presented in [137]. Several attacks were performed against the testbed, such as port scanner, address scan attack, device identification attack, device identification attack in aggressive mode, and exploit attack. After the data pre-processing, the final dataset consists of 6 features as the inputs of machine learning algorithms such as source port, total packets, total bytes, source packets, destination packets, and source bytes. The number of samples is 7,037,983, where each row is labeled as 0 or 1, denoting natural traffic or attack traffic, respectively.
- (c) *UNSW-IoT-Botnet-2018* [138]. The dataset³ was captured from *pcap* files with 69.3 GB in size and more than 72 million records. It was created by designing a realistic network environment, incorporating normal and botnet traffic. The dataset comprises multiple attacks such as DDoS, DoS, service scan, keylogging, and data exfiltration attacks. In this study, we used the compact version of the dataset, where it is only 5% of the original samples. The extracted 5% includes about three million records with 16 input features.

6.3 Evaluation Result and Discussion

The experiment is run on a machine with an Intel Xeon Gold 6240 2.6 GHz, 32GB RAM, and six NVIDIA Tesla V100 Volta GPUs. We use a non-resampling validation technique (e.g., hold-out), where the ratio between training and testing samples is 70:30. The models' predictive performances are estimated using an accuracy, F1, area under ROC curve (AUC), and area under precision-recall curve (AUCPR) which are better-suited for binary classification involving class imbalance problem [139]. In case of a binary classification problem, the above-mentioned performance metrics are formally defined as follows.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad (2)$$

¹ <https://bit.ly/38TGsbB>.

² <https://bit.ly/36NQ9WD>.

³ <https://bit.ly/3kPwMkG>.

Table 9 Summarization of primary studies by detection technique, domain of interest, and other relevant categories in 2019

Author(s)	Type	Tasks	Dataset	Performance metric	Remark
Zolanvari et al. [97]	Anomaly	Classification	Private	Accuracy, false positive rate, undetected rate, Matthews correlation coefficient, and sensitivity	High false positive rate
Zhou et al. [98]	Misuse	Classification	Private	Accuracy and AUC	Information fusion technique is further required
Smith et al. [99]	Anomaly	Classification	Private	Accuracy	Used a small sample set of PLCs
Derhab et al. [100]	Hybrid	Classification	Private	Accuracy and false positive rate	More ICSs attack datasets are further required
Yang et al. [101]	Misuse	Classification	Private	Precision and recall	Further evaluation against mixed attack types is necessary
Vavra and Hromada [112]	Anomaly	Optimization via genetic algorithm	SCADA network [124]	Not mentioned	Detection result was not clearly presented
Sokolov et al. [56]	Anomaly	Classification	Gas pipeline [120]	Accuracy, precision, and recall	Small traffic samples were used
Qassim et al. [46]	Anomaly	Cluster analysis	DARPA 1998	Not mentioned	Focused on a particular attack
Anton et al. [57]	Anomaly	Classification on imbalanced datasets	Gas pipeline [120]	Accuracy, precision, recall, and F_1	Validation on some types of attacks is necessary

$$F1 = \frac{2 \cdot TP}{2 \cdot TP + FP + FN} \quad (3)$$

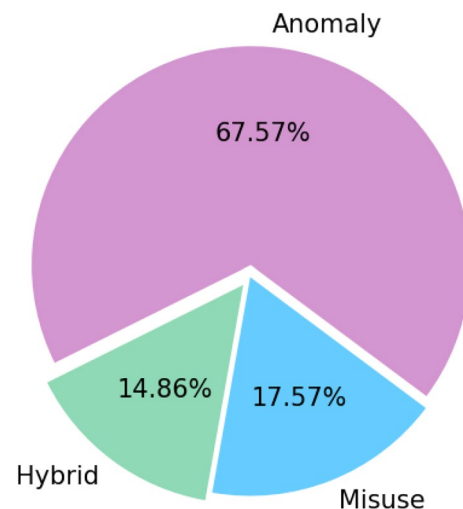
$$AUC = \int_0^1 \frac{TP}{P} d\frac{FP}{N} == \int_0^1 \frac{TP}{P} \left(\frac{FP}{N}\right)^{-1}(x) dx \quad (4)$$

where TP, TN, FP, and FN values can be obtained from a confusion matrix shown in Fig. 7. TN is not considered in AUCPR since when data is skewed, a high number of TNs often outweighs the impact of changes in other variables, such as FPs. Therefore, AUCPR is much sensitive to TPs, FPs, and FNs compared to AUC [140]. For the calculation of AUCPR, the interpolation between two points m and n in the AUCPR space is specified as a function:

$$y = \frac{TP_m + x}{\frac{TP_m + x + FP_m + ((FP_n - FP_m) \cdot x)}{TP_n - TP_m}} \quad (5)$$

where x is any real value between TP_m and TP_n .

We first show the performance scores of all benchmarked algorithms. Figure 8 compares the distribution of performance across multiple performance measures. The stacking ensemble outperforms the other techniques in all median scores except AUCPR. Additionally, there is a greater degree of fluctuation (e.g., dispersion) in the performance score of DNN, which exhibits a positive skew. It indicates that DNN is more unstable than any benchmarked algorithms. In comparison, the performance of the other algorithms, i.e.,

**Fig. 6** Dissemination of chosen studies according to three IDS technique categories, namely anomaly (i.e., binary class), misuse (i.e., multi class), and hybrid

XGBoost, RF, GBM, and Stacking exhibits less dispersion, indicating that they perform consistently across datasets.

Next, using the average performance score, hierarchical clustering was conducted on classifiers and datasets in order to better understand their relationships (see Fig. 9). The clustering task was completed using the Euclidean distance and Ward's clustering criterion. This experiment identified two and three major clusters for classifiers and datasets,

Table 10 Summarization of primary studies by detection technique, domain of interest, and other relevant categories in 2020

Author(s)	Type	Tasks	Dataset	Performance metric	Remark
Upadhyay et al. [69]	Hybrid	Classification	Power system	Accuracy, precision, FPR, recall, F_1	Applying majority ensemble vote method.
Süzen [102]	Anomaly	Classification	Private	Accuracy, TPR, FPR, AUC	Real-time detection is desirable.
Robles-Durazno et al. [103]	Anomaly	Classification	Private	Accuracy, FPR, FNR	High false alarm rate
Reuter et al. [113]	Misuse	Classification	CICIDS 2017	Precision, recall, F_1	The proposed model must be validated on a diverse SCADA datasets.
Renström et al. [104]	Anomaly	Classification	Private	Precision, recall	Why and when an anomaly occurred could be further investigated.
Ramotsoela et al. [114]	Misuse	Classification	BATADAL [125]	TPR, TNR, PPV, F_1	Generalization of the proposed model is still underexplored.
Radoglou-Grammatikis et al. [105]	Anomaly	Classification	Private	Accuracy, TPR, FPR, F_1	Other industrial application layer protocol will be investigated.
Priyanga et al. [76]	Anomaly	Classification	SWaT	Accuracy, precision, recall, F_1	Investigating attack at each stage and locate the targeted components of the dataset
Phillips et al. [58]	Anomaly	Classification	Gas pipeline	Accuracy, precision, recall, F_1	Evaluating ML algorithms with more complex SCADA systems.
Onoda [44]	Hybrid	Classification	Water storage, gas pipeline, DARPA	DR, FPR	Evaluating ML algorithms with more complex ICSs.
Neha et al. [77]	Anomaly	Classification	SWaT	DR, accuracy	The generalizability of the proposed model.
MR et al. [78]	Hybrid	Classification	SWaT	Accuracy, precision, recall, FPR, F_1	Multipoint attacks will be further investigated.
Mozaffari et al. [70]	Anomaly	Classification	Power system	Accuracy, precision, recall, F_1	The generalizability of the proposed model.
Liu et al. [59]	Anomaly	Classification	Water storage, gas pipeline	Accuracy, DR, FPR	The proposed model must be validated on a diverse SCADA datasets.
Lan et al. [106]	Anomaly	Classification	Private	Precision, recall, F_1	The generalizability of the proposed model.
Kim et al. [79]	Anomaly	Feature learning for dimensionality reduction	SWaT	RMSE	Real-time detection mechanism is required
Joshi et al. [60]	Anomaly	Feature learning and classification	Gas pipeline	Precision, recall, F_1	Explainability of the model is underexplored.
Hassan et al. [71]	Anomaly	Classification	Power system	Accuracy, FPR	Execution time and optimal random feature selection.
Hassan et al. [107]	Anomaly	Feature learning and classification	Private	Accuracy, precision, recall, F_1 , AUC	Adversarial deep learning model is not discussed.
Hallaji et al. [61]	Misuse	Classification	Gas pipeline	Accuracy	Real-time detection mechanism is not discussed.
Haghnegahdar and Wang [72]	Hybrid	Classification	Power system	Accuracy, precision, recall, F_1	Real-time detection mechanism is not discussed.
Gumaei et al. [73]	Hybrid	Classification	Power system	Accuracy, precision, recall, F_1	Wrapper and filter-based feature selection approaches are underexplored.

Table 10 (continued)

Author(s)	Type	Tasks	Dataset	Performance metric	Remark
Gao et al. [47]	Anomaly	Classification	Private, KDD Cup 99	Precision, recall, F_1	Applying the model for multi-attacks detection.
Elnour et al. [80]	Anomaly	Classification	SWaT	Accuracy, FPR	Higher FPR rate.
Egger et al. [108]	Hybrid	Classification	Private	AUC	More difficult attack vectors and more advanced ML algorithms will be further explored.
Demertzis et al. [62]	Anomaly	Clustering, classification	Gas pipeline, water storage, power system	Accuracy, precision, recall, F_1 , AUC	Online learning method using data stream will be further investigated.
Das et al. [81]	Anomaly	Classification	SWaT	Precision, recall, F_1	Detection on resource constrained device will be further explored.
Choubineh et al. [63]	Anomaly	Classification	Gas pipeline	Accuracy, FPR, TPR, F_1 , MCC	Multi-attacks detection is not discussed.
Chaithanya et al. [74]	Anomaly	Classification	Power system	Accuracy, DR	The generalizability of the proposed model.
Al-Abassi et al. [64]	Anomaly	Feature representations and classification	Gas pipeline, SWaT	Accuracy, precision, recall, F_1	Identifying different attack types and their location will be further explored.

Table 11 Event scenarios groups of power system dataset

Scenarios	Class labels
Attack events	7-12, 15-30, 35-40
Natural events	1-6, 13-14
No events	41

respectively. The clusters of classifiers are particularly robust, as the top and the worst-performing classifiers were grouped separately. Furthermore, the three clusters of datasets highlight the main peculiarities between datasets. For instance, one cluster consists of datasets with extremely low imbalance ratio value such as WUSTL SCADA and UNSW-IoT-BoTnet, while another cluster, on the other hand, contains datasets with relatively higher imbalance ratio scores (> 0.4) such as P6, P15, P12, P3, and P8.

Statistical tests are used to evaluate the performance results in accordance with the recommendation in [141]. For statistical significance, a Friedman test [142] was utilized, followed by the Nemenyi posthoc test [143] to verify the locations of statistically significant differences between classifiers. Statistical analysis results are typically presented as a critical difference plot [141]. The diagram depicts the average ranks of the classifiers and connect those whose average ranks are less than the critical difference. The critical difference is determined by the significance level (e.g., 0.05 in our case). In the first evaluation scenario, the Friedman omnibus test indicates that there is at least a highly significant performance difference ($p < 0.001$) between two algorithms across all performance metrics. We then apply posthoc test using

Nemenyi test and visualize the critical difference plot in Figure 10. Except for the AUC score, Stacking is obviously a top performer, outperforming other individual ensemble algorithms such as GBM, RF, XGBoost, and DNN across the board. In contrast, DNN has consistently performed poorly across all performance criteria.

As an important part of our study, we are interested in reporting the computational complexity of the benchmarked classifiers, particularly the time necessary for the training and testing tasks (see Tables 13, 14). In average, XGBoost requires shorter training time than other base learners, i.e., RF, GBM, and DNN, despite the fact that all base learners are trained using 10-fold cross validation. Stacking needs substantially less training effort than other methods as it merely involves basic matrix manipulation (e.g., collecting the prediction values from base classifiers). Furthermore, regardless of the size of the testing set, XGBoost obtained the quickest detection time with an average of 0.40 second.

7 Conclusion and Further Research Directions

The paper discussed a systematic mapping study that provided particular attention on carrying out a literature review of machine learning and deep learning algorithms for intrusion detection in ICSs environment. We conveyed our following RQs and served answers for them.

- (i) RQ_1 : What is the research trend in machine learning and deep learning-based intrusion detection in ICSs?

Table 12 The characteristics of the dataset utilized in the experiment

Dataset	# of attack samples	# of natural samples	Imbalance ratio
P1	3866	1100	0.285
P2	3525	1544	0.438
P3	3811	1604	0.421
P4	3402	1800	0.530
P5	3680	1481	0.402
P6	3490	1477	0.423
P7	3910	1326	0.339
P8	3771	1544	0.409
P9	3570	1770	0.496
P10	3921	1648	0.420
P11	3969	1282	0.323
P12	3453	1771	0.513
P13	4118	1153	0.280
P14	3762	1353	0.360
P15	3415	1861	0.450
WUSTL SCADA	6,634,581	403,402	0.061
UNSW-IoT-BoTnet	2,934,447	370	0.000013

		Prediction outcome		Total
		Normal	Anomaly	
Actual outcome	Normal	True Positive (TP)	False Negative (FN)	P'
	Anomaly	False Positive (FP)	True Negative (TN)	N'
Total		P	N	

Fig. 7 A confusion matrix with a binary-class focus

The research trend that we could observe is the use of various deep learning-based models, both in supervised and unsupervised learning tasks. Our results suggest that there has been a steep rise in applying ML and DL techniques for IDS on the industrial network started from 2017 onward.

- (ii) RQ_2 : What types of learning algorithms have been employed to deal with the problems of IDSs in industrial networks? The vast majority of the algorithm presented in this study is supervised learning. Sev-

eral classification techniques, such as SVM, RF, and KNN, are the most frequently utilized classifiers.

- (iii) RQ_3 : Which types of intrusion detection techniques are prevalently used in ICSs? According to our mapping study, an anomaly-based detection technique is commonly considered, which accounts for two-thirds of the total selected studies.
- (iv) RQ_4 : What are the relative performance of AI algorithms for ICS-based IDS? This study compares the relative performance of stacked generalization ensemble and several individual classifiers, i.e., RF, GBM, XGBoost, and DNN. On a binary classification task, it is demonstrated that the stacked generalization ensemble outperforms individual classifiers significantly.

Numerous potential extensions to the works presented here are as follows. First, according to our findings in Tables 6, 7, 8, 9 and 10, there is still a significant research gap in the use of AI algorithms in unsupervised and semi-supervised learning modes. More exactly, a deep learning technique, i.e., autoencoder, remains mostly unexplored due to the fact that just a few studies have utilized it thus far. Currently, there has been a tremendous progress in the application of deep learning models to tabular data [144, 145]. Therefore, further study is probably required in this area, particularly

to determine whether deep learning models perform statistically superior on tabular data. Second, as Zolanvari et al. [97] and Upadhyay et al. [127] pointed out, some features might degrade the accuracy of a machine learning algorithm; hence, taking the importance of the features into account is critical. The features are ranked based on how salient they are in contributing to the final prediction. Feature importance indicates how useful or valuable each feature was in the construction of the classification model. Lastly, there are limited number of benchmark datasets available for comparing the algorithms' performance. Hence, it is necessary to have a well-studied real-world or artificially generated ICS-based IDS datasets so that the performance comparison between algorithms can be fairly conducted.

Appendix A Nomenclature

AUC Area Under Receiver Operating Characteristic Curve
 CFS Correlation-based Feature Selection
 CNN Convolutional Neural Network
 DDoS Distributed Denial of Service
 DNN Deep Neural Network
 DoS Denial of Service
 DR Detection Rate
 FNR False Negative Rate
 FPR False Positive Rate
 GBM Gradient Boosting Machine
 GRU Gated Recurrent Unit
 IIoT Industrial Internet of Things
 LSTM Long Short-Term Memory

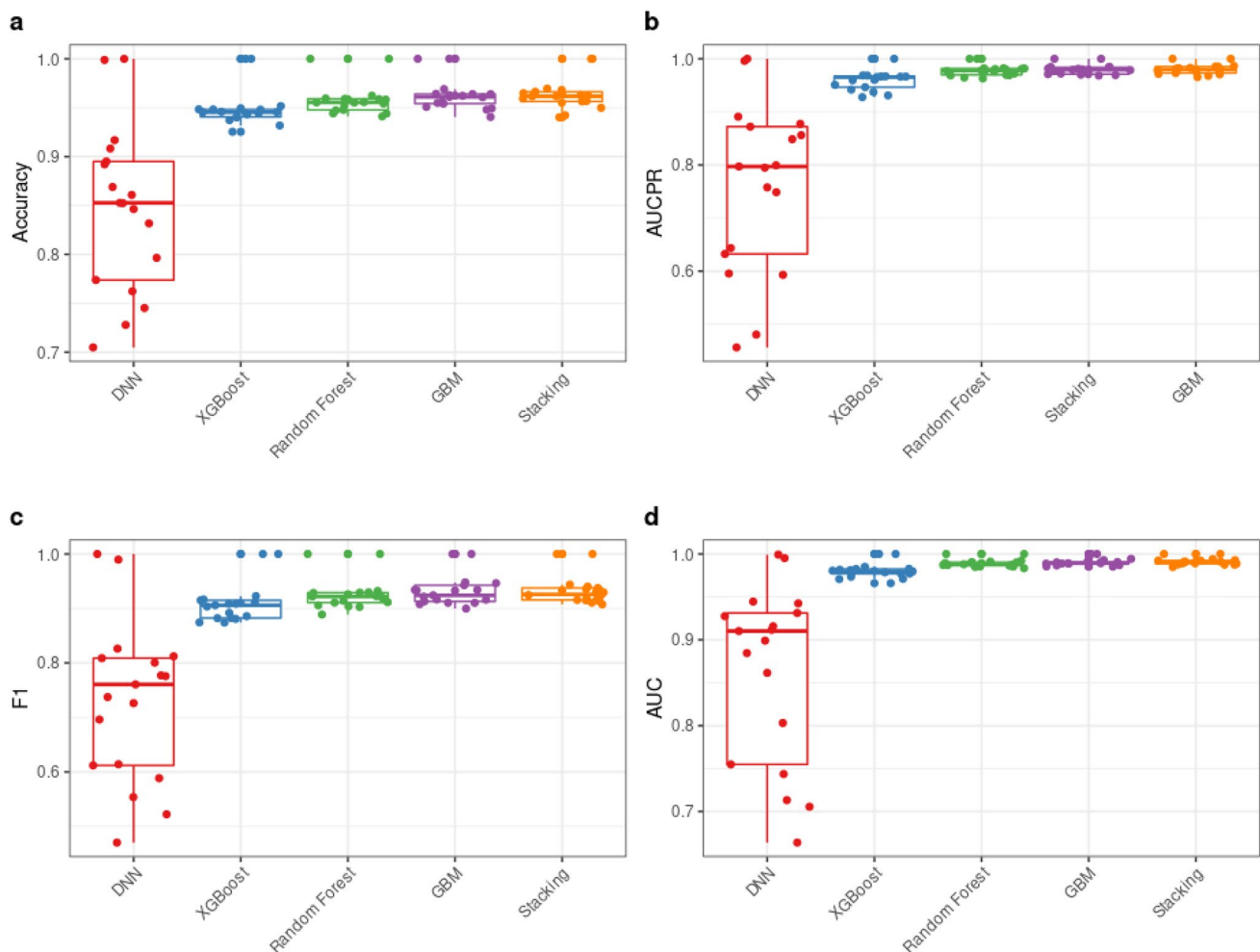


Fig. 8 Performance distribution of all benchmarked classifiers on all performance metrics, including accuracy (a), AUCPR (b), F1 (c), and AUC (d)

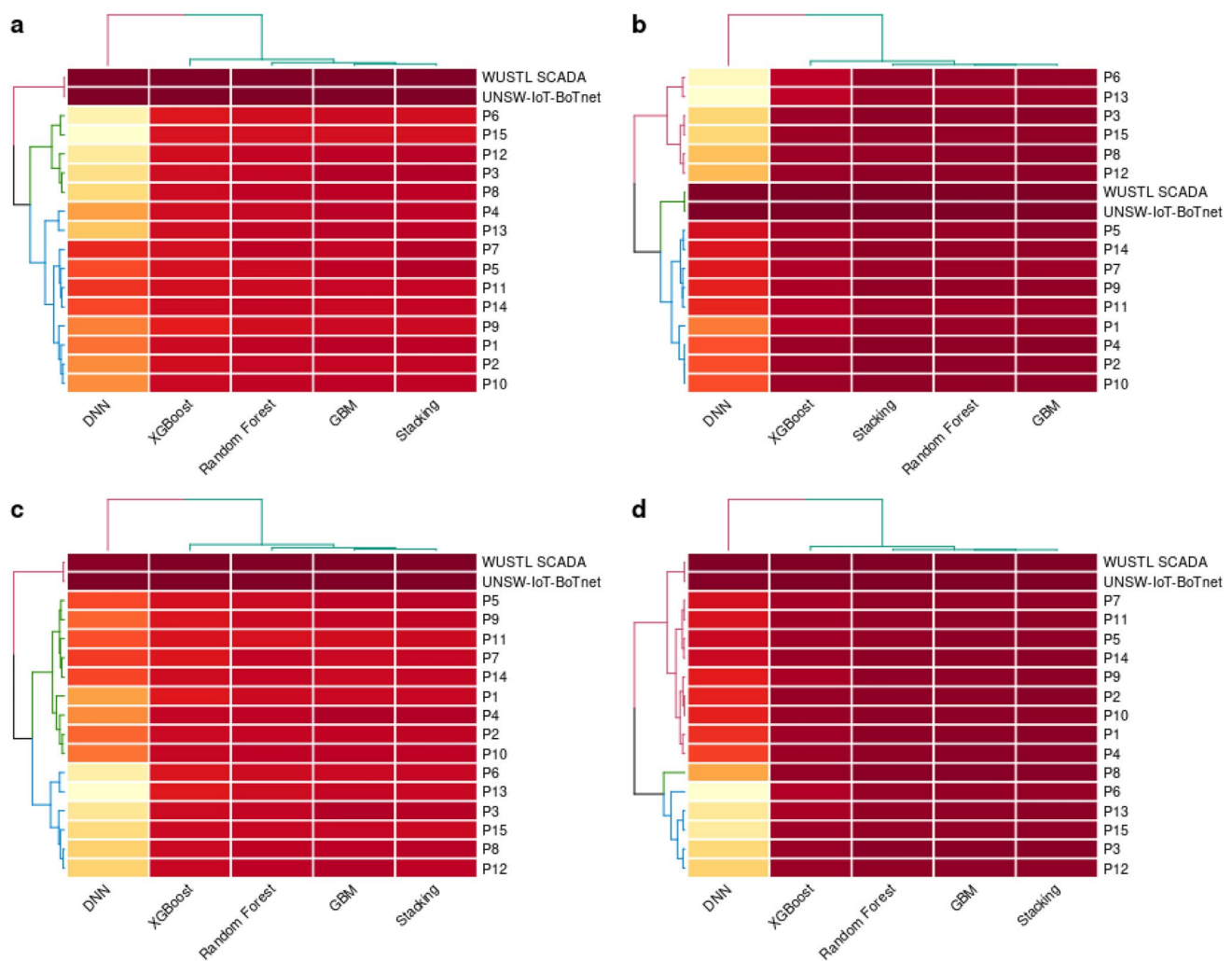


Fig. 9 Hierarchical clusters of algorithms and datasets according to their accuracy (**a**), AUCPR (**b**), F1 (**c**), and AUC (**d**) score. The clusters are represented by dendrogram branches in different colors

MCC Matthews Correlation Coefficient
 MLP Multi-layer Perceptron
 PCA Principle Component Analysis
 PPV Positive Predictive Value
 REPT Reduced Error Pruning Tree
 RF Random Forest

RMSE Root Mean Squared Error
 SVM Support Vector Machine
 TNR True Negative Rate
 TPR True Positive Rate
 XGBoost eXtreme Gradient Boosting

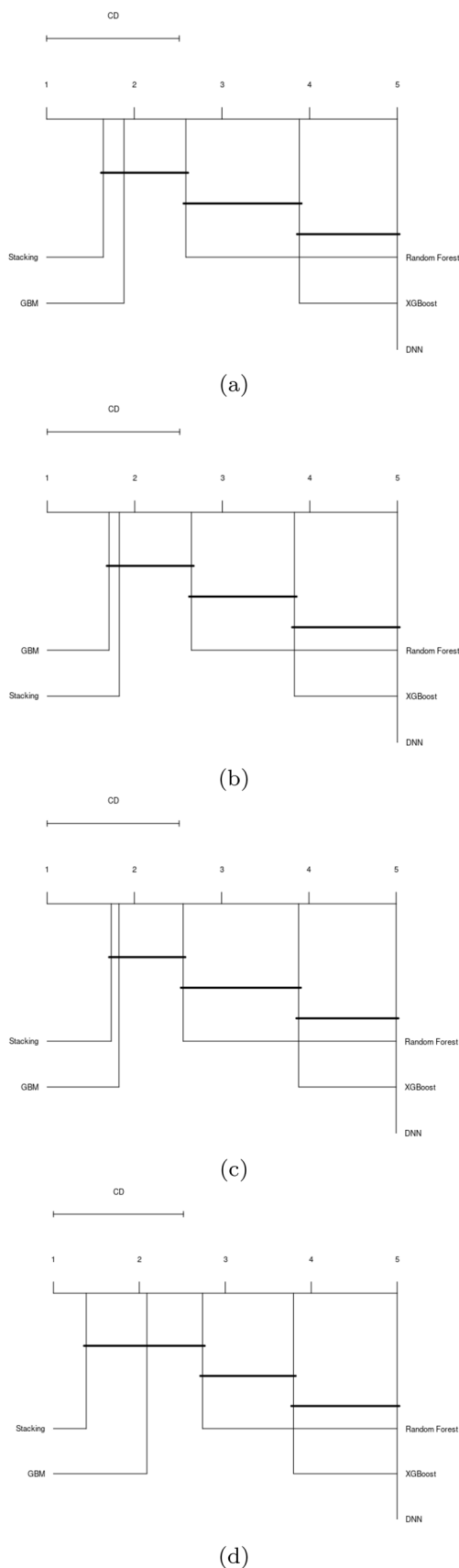


Fig. 10 Critical difference plot based on the Nemenyi posthoc test across all performance measures: **a** accuracy, **b** AUCPR, **c** F1, and **d** AUC

Table 13 The time taken by each classification algorithm to complete the training task on each dataset (in seconds)

Dataset	RF	GBM	XGBoost	DNN	Stacking
P1	2383.6	3044.5	46.4	857.9	2.4
P2	2187.4	3334.6	64.3	795.6	2.3
P3	2468.4	3500.2	52.3	983.8	3.5
P4	2302.2	3584.7	63.0	818.5	2.5
P5	2410.7	3362.5	52.3	967.6	3.5
P6	2290.9	2939.9	62.7	865.9	2.3
P7	2409.7	3305.4	53.4	1014.6	3.5
P8	2148.1	3238.3	63.4	918.5	2.3
P9	2556.2	3636.5	56.3	1150.7	3.5
P10	2348.9	3489.7	62.3	904.4	2.2
P11	2445.5	3252.6	54.4	872.4	3.5
P12	2247.1	3453.0	65.2	851.0	2.4
P13	2389.7	3369.2	52.3	1002.6	2.5
P14	2231.2	3455.1	56.1	873.3	2.3
P15	2463.0	3698.7	55.1	1187.2	3.5
WUSTL SCADA	1984.2	1841.5	2639.9	9108.8	9.4
UNSW-IoT-BoTnet	7088.7	8927.3	2149.5	2075.6	11.6
AVERAGE	2609.1	3613.8	332.3	1485.2	3.7

Table 14 The time taken by each classification algorithm to complete the testing task on each dataset (in seconds)

Dataset	RF	GBM	XGBoost	DNN	Stacking
P1	0.37	0.44	0.32	0.99	0.50
P2	0.41	0.39	0.40	0.38	0.46
P3	0.37	0.27	0.16	0.27	0.53
P4	0.52	0.45	0.33	0.34	0.80
P5	0.37	0.27	0.14	0.25	0.48
P6	0.30	0.28	0.25	0.33	0.44
P7	0.39	0.29	0.17	0.27	0.53
P8	0.30	0.30	0.23	0.23	0.46
P9	0.42	0.30	0.18	0.29	0.58
P10	0.61	0.38	0.33	0.36	0.48
P11	0.46	0.31	0.17	0.29	0.52
P12	0.36	0.35	0.29	0.28	0.50
P13	0.44	0.34	0.25	0.30	0.55
P14	0.43	0.34	0.27	0.30	0.49
P15	0.46	0.33	0.21	0.28	0.55
WUSTL SCADA	67.36	70.76	1.34	24.29	177.83
UNSW-IoT-BoTnet	39.93	76.11	1.74	66.60	41.79
AVERAGE	6.68	8.93	0.40	5.65	13.38

Acknowledgements This work was funded by the Institute for Basic Science (IBS), Republic of Korea under grant No. IBS-R029-C2-001. This work was also supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (MSIT) (No. 2020R1A2C1009744), in part by the Institute of Civil Military Technology Cooperation funded by the Defense Acquisition Program Administration and Ministry of Trade, Industry and Energy of the Korean government under grant No. 19-CM-GU-01, and in part by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) Grant funded by the Korean Government [Ministry of Trade, Industry, and Energy (MOTIE)] under Grant 20206610100290.

Declarations

Conflict of interest The authors declare that there is no conflict of interest in submitting this manuscript.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Galloway Brendan, Hancke Gerhard P (2012) Introduction to industrial control networks. *IEEE Commun Surveys Tutorials* 15(2):860–880
- Kim Dong-Seong, Tran-Dang Hoa (2019) An overview on industrial control networks. In *Industrial Sensors and Controls in Communication Networks*, pages 3–16. Springer
- Tao Fei, Cheng Jiangfeng, Qi Qinglin (2017) IIHub: An industrial internet-of-things hub toward smart manufacturing based on cyber-physical system. *IEEE Transact Indus Informat* 14(5):2271–2280
- Ferrari Paolo, Flammini Alessandra, Rinaldi Stefano, Sisinni Emiliano, Maffei Davide, Malara Matteo (2018) Impact of quality of service on cloud based industrial IoT applications with OPC UA. *Electronics* 7(7):109
- Abdo H, Kaouk M, Flaus J-M, Masse F (2018) A safety/security risk analysis approach of industrial control systems: A cyber bowtie-combining new version of attack tree with bowtie analysis. *Computers & Security* 72:175–195
- Gaiceanu Marian, Stanculescu Marilena, Andrei Paul Cristian, Solcanu Vasile, Gaiceanu Theodora, Andrei Horia (2020a) *Intrusion Detection on ICS and SCADA Networks*, pages 197–262. Springer
- Lin Chih-Ta, Wu Sung-Lin, Lee Mei-Lin (2017) Cyber attack and defense on industry control systems. In *IEEE Conference on Dependable and Secure Computing*, pages 524–526. IEEE. ISBN 150905569X
- Gonzalez Carlos Aguayo, Reed Jeffrey (2016) Cyber physical intrusion detection. In *Cyber-security of SCADA and Other Industrial Control Systems*, pages 239–251. Springer
- Meshram Ankush, Haas Christian (2017a) Anomaly detection in industrial networks using machine learning: A roadmap, pages 65–72. Springer
- Bayu Adhi Tama and Kyung-Hyune Rhee (2019) An in-depth experimental study of anomaly detection using gradient boosted machine. *Neural Computing and Applications* 31(4):955–965
- Maya Hilda Lestari Louk and Bayu Adhi Tama (2021) Exploring ensemble-based class imbalance learners for intrusion detection in industrial control networks. *Big Data and Cognitive Computing* 5(4):72
- Anderson James P (1980) *Computer security threat monitoring and surveillance*. Technical Report, James P. Anderson Company
- Adhi Tama Bayu, Sunghoon Lim (2021) Ensemble learning for intrusion detection systems: A systematic mapping study and cross-benchmark evaluation. *Comput Sci Rev* 39:100357
- LeCun Yann, Bengio Yoshua, Hinton Geoffrey (2015) Deep learning. *Nature* 521(7553):436–444
- Flaus Jean-Marie, Georgakis John (2018) Review of machine learning based intrusion detection approaches for industrial control systems. In *Computer & Electronics Security Applications Rendez-vous (C & ESAR) Conference*, pages 1–12
- Stouffler K, Pillitteri V, Lightman S, Abrams M, Hahn A (2015) NIST special publication 800-82 rev 2: Guide to industrial control systems (ICS) security
- Krotofil Maryna, Gollmann Dieter (2013) Industrial control systems security: What is happening? In *11th IEEE International Conference on Industrial Informatics (INDIN)*, pages 670–675. IEEE
- Weiss Joseph (2010) *Protecting industrial control systems from electronic threats*. Momentum Press, New York
- Bolton William (2015) *Programmable logic controllers*. Newnes, London
- Koucham Oualid (2018) *Intrusion detection for industrial control systems*. PhD thesis, Université Grenoble Alpes
- Liao Hung-Jen, Lin Chun-Hung Richard, Lin Ying-Chih, Tung Kuang-Yuan (2013) Intrusion detection system: a comprehensive review. *J Net Comput Appl* 36(1):16–24
- Valdes Alfonso, Anderson Debra (1995) Statistical methods for computer usage anomaly detection using NIDES (next-generation intrusion detection expert system). In *3rd International Workshop on Rough Sets and Soft Computing*, pages 306–311
- Ghosh Anup K, Wanken James, Charron Frank (1998) Detecting anomalous and unknown intrusions against programs. In *14th Annual Computer Security Applications Conference*, pages 259–267. IEEE
- Primartha Rifkie, Tama Bayu Adhi (2017) Anomaly detection using random forest: A performance revisited. In *International Conference on Data and Software Engineering (ICoDSE)*, pages 1–6. IEEE
- Vigna Giovanni, Kemmerer Richard A (1998) Netstat: A network-based intrusion detection approach. In *14th Annual Computer Security Applications Conference*, pages 25–34. IEEE
- Gaiceanu Marian, Stanculescu Marilena, Andrei Paul Cristian, Solcanu Vasile, Gaiceanu Theodora, Andrei Horia (2020b) *Intrusion detection on ICS and SCADA networks*. In *Recent Developments on Industrial Control Systems Resilience*, pages 197–262. Springer
- Yan Hu, Yang An, Li Hong, Sun Yuyan, Sun Limin (2018) A survey of intrusion detection on industrial control systems. *Int J Dist Sensor Net* 14(8):1550147718794615
- Kaouk Mohamad, Flaus Jean-Marie, Potet Marie-Laure, Groz Roland (2019) A review of intrusion detection systems for industrial control systems. In *6th International Conference on Control, Decision and Information Technologies (CoDIT)*, pages 1699–1704. IEEE

29. Jiang Dianbin, Zhao Jingling (2019) Machine learning in industrial control system security: A survey. In Chinese Intelligent Systems Conference, pages 310–317. Springer
30. Zhu Bonnie, Sastry Shankar (2010) SCADA-specific intrusion detection/prevention systems: a survey and taxonomy. In Proceedings of the 1st workshop on secure control systems (SCS), volume 11, page 7
31. Meshram Ankush, Haas Christian (2017b) Anomaly detection in industrial networks using machine learning: A roadmap. In Machine Learning for Cyber Physical Systems, pages 65–72. Springer
32. Petersen Kai, Feldt Robert, Mujtaba Shahid, Mattsson Michael (2008) Systematic mapping studies in software engineering. In International Conference on Evaluation and Assessment in Software Engineering 8:68–77
33. Petersen Kai, Vakkalanka Sairam, Kuzniarz Ludwik (2015) Guidelines for conducting systematic mapping studies in software engineering: An update. *Inf Soft Technol* 64:1–18
34. Kitchenham Barbara Ann, Budgen David, Brereton Pearl (2015) Evidence-based software engineering and systematic reviews, volume 4. CRC press
35. Ratan Simmi K, Anand Tanu, Ratan John (2019) Formulation of research question-stepwise approach. *J Indian Association of Pediatric Surgeons* 24(1):15
36. Myers David, Suriadi Suriadi, Radke Kenneth, Foo Ernest (2018) Anomaly detection for industrial control systems using process mining. *Computers & Security*, 78:103–125. ISSN 0167-4048
37. Kang BooJoong, McLaughlin Kieran, Sezer Sakir (2016) Towards a stateful analysis framework for smart grid network intrusion detection. In 4th International Symposium for ICS & SCADA Cyber Security Research, pages 124–131
38. Jardine William, Frey Sylvain, Green Benjamin, Rashid Awais (2016) Senami: Selective non-invasive active monitoring for ics intrusion detection. In Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, pages 23–34
39. Ghaeini Hamid Reza, Tippenhauer Nils Ole (2016) Hamids: hierarchical monitoring intrusion detection system for industrial control systems. In Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, pages 103–111. ACM. ISBN 1450345689
40. Yüksel Ömer, den Hartog Jerry, Etalle Sandro (2016) Reading between the fields: practical, effective intrusion detection for industrial control systems. In Proceedings of the 31st Annual ACM Symposium on Applied Computing, pages 2063–2070
41. Potluri S, Henry NF, Diedrich C (2017) Evaluation of hybrid deep learning techniques for ensuring security in networked control systems. In 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), pages 1–8. ISBN 1946-0759
42. Potluri Sasanka, Diedrich Christian (2017) Deep feature extraction for multi-class intrusion detection in industrial control systems. *Int J Comput Theory Eng* 9(5):374–379
43. Zong Xuejun, Sun Yongchao, He Kan (2018) Intrusion detection based on traffic research and application in industrial control system. *Science, Engineering & Education* 3(1):17–22
44. Onoda Takashi (2020) Machine Learning Based Intrusion Detection in Control System Communication. In Design and Analysis of Distributed Energy Management Systems, pages 167–202. Springer
45. Samdarshi R, Sinha N, Tripathi P (2015) A triple layer intrusion detection system for scada security of electric utility. In Annual IEEE India Conference (INDICON), pages 1–5. ISBN 2325-9418. <https://doi.org/10.1109/INDICON.2015.7443439>
46. Qassim QS, Ahmad AR, Ismail R, Abu Bakar A, Abdul Rahim F, Mokhtar MZ, Ramli R, Mohd Yusof B, Mahdi MN (2019) An anomaly detection technique for deception attacks in industrial control systems. In IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), pages 267–272. ISBN null
47. Gao Jun, Gan Luyun, Buschendorf Fabiola, Zhang Liao, Liu Hua, Li Peixue, Dong Xiaodai, Lu Tao (2020) Omni SCADA intrusion detection using deep learning algorithms. *IEEE Internet of Things Journal*. ISSN 2327-4662
48. Beaver JM, Borges-Hink RC, Buckner MA (2013) An evaluation of machine learning methods to detect malicious scada communications. In 12th International Conference on Machine Learning and Applications, 2: 54–59
49. Nader P, Honeine P, Beausery P (2014) l_p -norms in one-class classification for intrusion detection in scada systems. *IEEE Transactions on Industrial Informatics* 10(4):2308–2317. <https://doi.org/10.1109/TII.2014.2330796>
50. Stefanidis Kyriakos, Voyiatzis Artemios G (2016) An hmm-based anomaly detection approach for scada systems. In IFIP International Conference on Information Security Theory and Practice, pages 85–99. Springer
51. Ullah I, Mahmoud QH (2017) A hybrid model for anomaly-based intrusion detection in scada networks. In IEEE International Conference on Big Data (Big Data), pages 2160–2167. ISBN null
52. Li Jinle, Wang Huazhong, Yan Bingyong (2017) Application of velocity adaptive shuffled frog leaping bat algorithm in ics intrusion detection. In 29th Chinese Control And Decision Conference (CCDC), pages 3630–3635. IEEE. ISBN 1509046577
53. Demertzis Konstantinos, Iliadis Lazaros, Spartalis Stefanos (2017) A spiking one-class anomaly detection framework for cyber-security on industrial control systems. In International Conference on Engineering Applications of Neural Networks, pages 122–134. Springer
54. Lopez Perez R, Adamsky F, Souza R, Engel T (2018) Machine learning for reliable network attack detection in SCADA systems. In 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pages 633–638. ISBN 2324-9013
55. Yang H, Zhou Z (2018) A novel intrusion detection scheme using cloud grey wolf optimizer. In 37th Chinese Control Conference (CCC), pages 8297–8302. ISBN 1934-1768
56. Sokolov AN, Alabugin SK, Pyatnitsky IA (2019) Traffic modeling by recurrent neural networks for intrusion detection in industrial control systems. In International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), pages 1–5. ISBN null
57. Anton Simon D Duque, Sinha Sapna, Schotten Hans Dieter (2019) Anomaly-based intrusion detection in industrial data with SVM and random forests. In International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pages 1–6. IEEE
58. Phillips Brandon, Gamess Eric, Krishnaprasad Sri (2020) An Evaluation of Machine Learning-based Anomaly Detection in a SCADA System Using the Modbus Protocol. In Proceedings of the 2020 ACM Southeast Conference, pages 188–196
59. Liu Huipeng, Zhou Zhiping, Zhang Min (2020) Application of optimized bidirectional generative adversarial network in ICS intrusion detection. In Chinese Control And Decision Conference (CCDC), pages 3009–3014. IEEE
60. Joshi Chaitali, Khochare Janavi, Rathod Jash, Kazi Faruk (2020) A Semi-Supervised Approach for Detection of SCADA Attacks in Gas Pipeline Control Systems. In IEEE-HYDICON, pages 1–8. IEEE. ISBN 1-72814-994-0
61. Hallaji Ehsan, Razavi-Far Roozbeh, Saif Mehrdad (2020) Detection of Malicious SCADA Communications via Multi-Subspace

- Feature Selection. In *International Joint Conference on Neural Networks (IJCNN)*, pages 1–8. IEEE. ISBN 1-72816-926-7
62. Konstantinos Demertzis, Lazaros Iliadis, Ilias Bougoudis (2020) Gryphon: a semi-supervised anomaly detection system based on one-class evolving spiking neural network. *Neural Comput Appl* 32(9):4303–4314
 63. Choubineh Abouzar, Wood David A, Choubineh Zahak (2020) Applying Separately Cost-sensitive Learning and Fisher's Discriminant Analysis to Address the Class Imbalance Problem: A Case Study Involving a Virtual Gas Pipeline SCADA System. *International Journal of Critical Infrastructure Protection*, page 100357. ISSN 1874-5482
 64. Abdulrahman Al-Abassi, Hadis Karimipour, Ali Dehghan-tanha, Parizi Reza M (2020) An ensemble deep learning-based cyber-attack detection in industrial control system. *IEEE Access* 8:83965–83973
 65. Almalawi Abdulmohsen Yu, Xinghuo Tari Zahir, Adil Fahad, Ibrahim Khalil (2014) An unsupervised anomaly-based detection approach for integrity attacks on scada systems. *Computers & Security* 46:94–110
 66. Tomlin L, Farnam Marsella R, Pan Shengyi (2016) A clustering approach to industrial network intrusion detection. In *Proceedings of the 2016 Information Security Research and Education (INSuRE) Conference (INSuRECon-16)*, pages 1–6
 67. Vávra Jan, Hromada Martin (2017) Anomaly detection system based on classifier fusion in ICS environment. In *International Conference on Soft Computing, Intelligent System and Information Technology (ICSIT)*, pages 32–38. IEEE. ISBN 1467398993
 68. Chen X, Zhang L, Liu Y, Tang C (2018) Ensemble learning methods for power system cyber-attack detection. In *IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, pages 613–616. ISBN null
 69. Upadhyay Darshana, Manero Jaume, Zaman Marzia, Sampalli Srinivas (2020a) Gradient Boosting Feature Selection with Machine Learning Classifiers for Intrusion Detection on Power Grids. *IEEE Transactions on Network and Service Management*. ISSN 1932-4537
 70. Mozaffari Farnaz Seyyed, Karimipour Hadis, Parizi Reza M (2020) Learning based anomaly detection in critical cyber-physical systems. In *Security of cyber-physical systems*, pages 107–130. Springer
 71. Mehedi Hassan Mohammad, Abdu Gumaei, Shamsul Huda, Ahmad Almogren (2020) Increasing the Trustworthiness in the Industrial IoT Networks Through a Reliable Cyberattack Detection Model. *IEEE Transactions on Industrial Informatics* 16(9):6154–6162
 72. Lida Haghnegahdar, Yong Wang (2020) A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection. *Neural Comput Appl* 32(13):9427–9441
 73. Abdu Gumaei, Mehedi Hassan Mohammad, Shamsul Huda, Rafiul Hassan Md, David Camacho, Javier Del Ser, Giancarlo Fortino (2020) A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids. *Applied Soft Computing* 96:106658
 74. Chaithanya PS, Priyanga S, Pravinraj S, Sriram VS Shankar (2020) SSO-IF: An Outlier Detection Approach for Intrusion Detection in SCADA Systems. In *Inventive Communication and Computational Technologies*, pages 921–929. Springer
 75. Kravchik Moshe, Shabtai Asaf (2018) Detecting cyber attacks in industrial control systems using convolutional neural networks. In *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy*, pages 72–83
 76. S Priyanga, Kannan Krithivasan, S Pravinraj, and Shankar Sriram VS. Detection of Cyberattacks in Industrial Control systems using Enhanced Principal Component Analysis and Hypergraph based Convolution Neural Network (EPCA-HG-CNN). *IEEE Transactions on Industry Applications*, 2020. ISSN 0093-9994
 77. Neha N, Priyanga S, Seshan Suresh, Senthilnathan R, Sriram VS Shankar (2020) SCO-RNN: A Behavioral-Based Intrusion Detection Approach for Cyber Physical Attacks in SCADA Systems. In *Inventive Communication and Computational Technologies*, pages 911–919. Springer
 78. Gauthama Raman MR, Nivethitha Somu, Mathur AP (2020) A Multilayer Perceptron Model for Anomaly Detection in Water Treatment Plants. *International Journal of Critical Infrastructure Protection*, page 100393. ISSN 1874-5482
 79. SungJin Kim, WooYeon Jo, Taeshik Shon (2020) APAD: Autoencoder-based Payload Anomaly Detection for industrial IoT. *Appl Soft Comput* 88:106017
 80. Elnour Mariam, Meskin Nader, Khan Khlaed M (2020) Hybrid Attack Detection Framework for Industrial Control Systems using 1D-Convolutional Neural Network and Isolation Forest. In *IEEE Conference on Control Technology and Applications (CCTA)*, pages 877–884. IEEE. ISBN 1-72817-140-7
 81. Das Tanmoy Kanti, Adepu Sridhar, Zhou Jianying (2020) Anomaly Detection in Industrial Control Systems using Logical Analysis of Data. *Computers & Security*, page 101935. ISSN 0167-4048
 82. Stanislav Ponomarev, Travis Atkison (2015) Industrial control system network intrusion detection by telemetry analysis. *IEEE Transact Depend Secure Comput* 13(2):252–260
 83. Hoscic Jasenko, Lamps Jerome, Hart Derek H (2015) Evolving decision trees to detect anomalies in recurrent ics networks. In *World Congress on Industrial Control Systems Security (WCICSS)*, pages 50–57. IEEE. ISBN 1908320583
 84. Abdullah Khalili, Ashkan Sami (2015) Sysdetect: a systematic approach to critical state determination for industrial intrusion detection systems using apriori algorithm. *J Process Control* 32:154–160
 85. Ponomarev Stanislav, Atkison Travis (2016) Session duration based feature extraction for network intrusion detection in control system networks. In *International Conference on Computational Science and Computational Intelligence (CSCI)*, pages 892–896. IEEE. ISBN 150905510X
 86. Eigner O, Kreimel P, Tavolato P (2016) Detection of man-in-the-middle attacks on industrial control networks. In *International Conference on Software Security and Assurance (ICSSA)*, pages 64–69. ISBN null. <https://doi.org/10.1109/ICSSA.2016.19>
 87. Terai Asuka, Abe Shingo, Kojima Shoya, Takano Yuta, Koshijima Ichiro (2017) Cyber-attack detection for industrial control system monitoring with support vector machine based on communication profile. In *IEEE European Symposium on Security and Privacy Workshops (EuroS & PW)*, pages 132–138. IEEE. ISBN 1538622440
 88. Li H, Qin S (2017) Optimization and implementation of industrial control system network intrusion detection by telemetry analysis. In *3rd IEEE International Conference on Computer and Communications (ICCC)*, pages 1251–1254. ISBN null
 89. Kreimel Philipp, Eigner Oliver, Tavolato Paul (2017) Anomaly-based detection and classification of attacks in cyber-physical systems. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, pages 1–6
 90. Francia GA (2017) A machine learning test data set for continuous security monitoring of industrial control systems. In *IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER)*, pages 1043–1048. ISBN null
 91. He X, Zhang L, Liu T, Wang W (2018) Detecting anomalies in distributed control systems by modeling traffic behaviors. In *IEEE 4th International Conference on Computer and Communications (ICCC)*, pages 534–538. ISBN null

92. Zolanvari M, Teixeira MA, Jain R (2018) Effect of imbalanced datasets on security of industrial iot using machine learning. In IEEE International Conference on Intelligence and Security Informatics (ISI), pages 112–117. ISBN null
93. Liu J, Yin L, Hu Y, Lv S, Sun L (2018) A novel intrusion detection algorithm for industrial control systems based on cnn and process state transition. In IEEE 37th International Performance Computing and Communications Conference (IPCCC), pages 1–8. ISBN 1097-2641
94. Schuster F, Kopp FM, Paul A, König H (2018) Attack and fault detection in process control communication using unsupervised machine learning. In IEEE 16th International Conference on Industrial Informatics (INDIN), pages 433–438. ISBN 2378-363X
95. Hong Ki-Seob, Kim Hyo-Bin, Kim Dong-Hyun, Seo Jung-Taek (2018) Detection of replay attack traffic in ICS network. In International Conference on Applied Computing and Information Technology, pages 124–136. Springer
96. Teixeira Marcio, Salman Tara, Zolanvari Maede, Jain Raj, Meskin Nader, Samaka Mohammed (2018) SCADA system testbed for cybersecurity research using machine learning approach. *Future Internet* 10(8):76
97. Zolanvari M, Teixeira MA, Gupta L, Khan KM, Jain R (2019) Machine learning-based network vulnerability analysis of industrial internet of things. *IEEE Internet of Things Journal* 6(4):6822–6834
98. Zhou M, Lv S, Yin L, Chen X, Li H, Sun L (2019) SCTM: A multi-view detecting approach against industrial control systems attacks. In IEEE International Conference on Communications (ICC), pages 1–6. ISBN 1550-3607
99. Smith Angela, Wedgbury Adam, Biondi Philippe, Soulsby Hugh, Jones Kevin (2019) Industrial control system defence: Debugging ICS maintenance network traffic. In 6th International Symposium for ICS & SCADA Cyber Security Research, pages 11–20
100. Abdelouahid Derhab, Mohamed Guerroumi, Abdu Gumaiei, Leandros Maglaras, Amine Ferrag Mohamed, Mithun Mukherjee, Aslam Khan Farrukh (2019) Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security. *Sensors* 19(14):3119
101. Yang H, Cheng L, Chuah MC (2019) Deep-learning-based network intrusion detection for SCADA systems. In IEEE Conference on Communications and Network Security (CNS), pages 1–7. ISBN null
102. Süzen Ahmet Ali (2020) Developing a multi-level intrusion detection system using hybrid-DBN. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–11. ISSN 1868-5145
103. Robles-Durazno Andres, Moradpoor Naghmeh, McWhinnie James, Russell Gordon (2020) Real-time anomaly intrusion detection for a clean water supply system, utilising machine learning with novel energy-based features. In International Joint Conference on Neural Networks (IJCNN), pages 1–8. IEEE. ISBN 1-72816-926-7
104. Renström Niklas, Bangalore Pramod, Highcock Edmund (2020) System-wide anomaly detection in wind turbines using deep autoencoders. *Renewable Energy*. ISSN 0960-1481
105. Radoglou-Grammatikis Panagiotis, Sarigiannidis Panagiotis, Efsthopoulos George, Karypidis Paris-Alexandros, Sarigiannidis Antonios (2020) DIDEROT: an intrusion detection and prevention system for DNP3-based SCADA systems. In Proceedings of the 15th International Conference on Availability, Reliability and Security, pages 1–8
106. Lan Haiyan, Zhu Xiaodong, Sun Jianguo, Li Sizhao (2020) Traffic Data Classification to Detect Man-in-the-Middle Attacks in Industrial Control System. In 2019 6th International Conference on Dependable Systems and Their Applications (DSA), pages 430–434. IEEE. ISBN 1-72816-057-X
107. Hassan Mohammad, Huda Shamsul, Sharmeen Shaila, Abawajy Jemal, Fortino Giancarlo (2020b) An adaptive trust boundary protection for IIoT networks using deep-learning feature extraction based semi-supervised model. *IEEE Transactions on Industrial Informatics*. ISSN 1551-3203
108. Egger Michael, Eibl Günther, Engel Dominik (2020) Comparison of approaches for intrusion detection in substations using the IEC 60870-5-104 protocol. *Energy Informatics*, 3(1):1–17
109. Mantere Matti, Sailio Mirko, Noponen Sami (2014) A module for anomaly detection in ics networks. In Proceedings of the 3rd international conference on High confidence networked systems, pages 49–56
110. Shamsul Huda, Suruz Miah, John Yearwood, Sultan Alyahya, Hmood Al-Dossari, Robin Doss (2018) A malicious threat detection model for cloud assisted internet of things (CoT) based industrial control system (ICS) networks using deep belief network. *J Parall Distrib Comp* 120:23–31
111. Yang A, Wang X, Sun Y, Hu Y, Shi Z, Sun L (2018) Multi-dimensional data fusion intrusion detection for stealthy attacks on industrial control systems. In IEEE Global Communications Conference (GLOBECOM), pages 1–7. ISBN 1930-529X
112. Vavra Jan, Hromada Martin (2019) Optimization of the novelty detection model based on LSTM autoencoder for ICS environment. In Intelligent Systems Applications in Software Engineering, pages 306–319. Springer International Publishing. ISBN 978-3-030-30329-7
113. Reuter Lenhard, Jung Oliver, Magin Julian (2020) Neural network based anomaly detection for SCADA systems. In 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), pages 194–201. IEEE. ISBN 1-72815-127-9
114. Daniel Ramotsoela Tsotspe, Petrus Hancke Gerhard, Abu-Mahfouz Adnan M (2020) Behavioural Intrusion Detection in Water Distribution Systems Using Neural Networks. *IEEE Access* 8:190403–190416
115. Mitchell Thomas M et al (1997) Machine learning. McGraw-Hill, Inc., New York, NY, USA
116. James Gareth, Witten Daniela, Hastie Trevor, Tibshirani Robert (2013) An introduction to statistical learning, volume 112. Springer
117. Zhou Zhi-Hua (2012) Ensemble methods: foundations and algorithms. Chapman and Hall/CRC, London
118. Morris Thomas, Srivastava Anurag, Reaves Bradley, Gao Wei, Pavurapu Kalyan, Reddi Ram (2011) A control system testbed to validate critical infrastructure protection concepts. *Int J Critical Infrastruct Prot* 4(2):88–103
119. Pan Shengyi, Morris Thomas, Adhikari Uttam (2015) Developing a hybrid intrusion detection system using data mining for power systems. *IEEE Transactions on Smart Grid* 6(6):3104–3113
120. Morris Thomas H, Thornton Zach, Turnipseed Ian (2015) Industrial control system simulation and data logging for intrusion detection system research. 7th annual southeastern cyber security summit, pages 3–4
121. Tavallaee Mahbod, Bagheri Ebrahim, Lu Wei, Ghorbani Ali A (2009) A detailed analysis of the kdd cup 99 data set. In 2009 IEEE symposium on computational intelligence for security and defense applications, pages 1–6. IEEE
122. Goh Jonathan, Adepu Sridhar, Junejo Khurum Nazir, Mathur Aditya (2016) A dataset to support research in the design of secure water treatment systems. In International Conference on Critical Information Infrastructures Security, pages 88–99. Springer
123. Shamsul Huda, Suruz Miah, Mehedi Hassan Mohammad, Rafiqul Islam, John Yearwood, Majed Alrubaian, Ahmad Almogren (2017) Defending unknown attacks on cyber-physical systems by semi-supervised approach and available unlabeled data. *Information Sciences* 379:211–228

124. Lemay Antoine, Fernandez José M (2016) Providing SCADA network data sets for intrusion detection research. In 9th Workshop on Cyber Security Experimentation and Test (CSET16), pages 1–8
125. Riccardo Taormina, Stefano Galelli, Ole Tuppenhauer Nils, Elad Salomons, Avi Ostfeld, Eliades Demetrios G, Mohsen Aghashahi, Raanju Sundararajan, Mohsen Pourahmadi, Katherine Banks M et al (2018) Battle of the attack detection algorithms: Disclosing cyber attacks on water distribution networks. *J Water Res Plann Manag* 144(8):04018048
126. Upadhyay Darshana, Manero Jaume, Zaman Marzia, Sampalli Srinivas (2020) Gradient boosting feature selection with machine learning classifiers for intrusion detection on power grids. *IEEE Transactions on Network and Service Management* 18(1):1104–1116
127. Upadhyay Darshana, Manero Jaume, Zaman Marzia, Sampalli Srinivas (2021) Intrusion detection in scada based power grids: Recursive feature elimination model with majority vote ensemble algorithm. *IEEE Transac Net Sci Eng* 8(3):2559–2574
128. Van der Laan Mark J, Polley Eric C, Hubbard Alan E (2007) Super learner. *Statistical applications in genetics and molecular biology*, 6(1)
129. Breiman Leo (1996) Stacked regressions. *Machine learning* 24(1):49–64
130. Candel Arno, Parmar Viraj, LeDell Erin, Arora Anisha (2016) Deep learning with h2o. H2O. ai Inc
131. Bergstra James, Bengio Yoshua (2012) Random search for hyperparameter optimization. *J Mac Learn Res* 13(1):281–305
132. Breiman Leo (2001) Random forests. *Machine learning* 45(1):5–32
133. Friedman Jerome H (2001) Greedy function approximation: a gradient boosting machine. *Annals of statistics*, pages 1189–1232
134. Chen Tianqi, Guestrin Carlos (2016) Xgboost: A scalable tree boosting system. In *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining*, pages 785–794
135. Morris Thomas, Gao Wei (2014) Industrial control system traffic data sets for intrusion detection research. In *International Conference on Critical Infrastructure Protection*, pages 65–78. Springer
136. Pan Shengyi, Morris Thomas, Adhikari Uttam (2015) Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data. *IEEE Transac Indus Informat* 11(3):650–662
137. Andrey Teixeira Marcio, Tara Salman, Maede Zolanvari, Raj Jain, Nader Meskin, Mohammed Samaka (2018) Scada system testbed for cybersecurity research using machine learning approach. *Future Internet* 10(8):76
138. Koroniotis Nickolaos, Moustafa Nour, Sitnikova Elena, Turnbull Benjamin (2019) Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Generation Computer Systems* 100:779–796
139. Davis Jesse, Goadrich Mark (2006) The relationship between precision-recall and roc curves. In *Proceedings of the 23rd international conference on Machine learning*, pages 233–240
140. Saito Takaya, Rehmsmeier Marc (2015) The precision-recall plot is more informative than the roc plot when evaluating binary classifiers on imbalanced datasets. *PloS One* 10(3):e0118432
141. Demšar Janez (2006) Statistical comparisons of classifiers over multiple data sets. *J Mach Learning Res* 7(Jan):1–30
142. Friedman Milton (1940) A comparison of alternative tests of significance for the problem of m rankings. *Ann Mathemat Stat* 11(1):86–92
143. Nemenyi Peter (1962) Distribution-free multiple comparisons. *Biometrics* 18(2):263
144. Shwartz-Ziv Ravid, Armon Amitai (2022) Tabular data: Deep learning is not all you need. *Information Fusion* 81:84–90
145. Borisov Vadim, Leemann Tobias, Seßler Kathrin, Haug Johannes, Pawelczyk Martin, Kasneci Gjergji (2021) Deep neural networks and tabular data: A survey. *arXiv preprint [arXiv:2110.01889](https://arxiv.org/abs/2110.01889)*

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.