sustainability

MDPI

Review

A Review of Research Works on Supervised Learning Algorithms for SCADA Intrusion Detection and Classification

Oyeniyi Akeem Alimi [1,*], Khmaies Ouahada [1], Adnan M. Abu-Mahfouz [1,2], Suvendi Rimer [1] and Kuburat Oyeranti Adefemi Alimi [1]

[1] Department of Electrical & Electronic Engineering Science, University of Johannesburg, Johannesburg 2006, South Africa; kouahada@uj.ac.za (K.O.); a.abumahfouz@ieee.org (A.M.A.-M.); suvendir@uj.ac.za (S.R.); kadefemi@uj.ac.za (K.O.A.A.)

[2] Council for Scientific and Industrial Research, Pretoria 0001, South Africa

* Correspondence: oalimi@uj.ac.za; Tel.: +27-738029570

Abstract: Supervisory Control and Data Acquisition (SCADA) systems play a significant role in providing remote access, monitoring and control of critical infrastructures (CIs) which includes electrical power systems, water distribution systems, nuclear power plants, etc. The growing interconnectivity, standardization of communication protocols and remote accessibility of modern SCADA systems have contributed massively to the exposure of SCADA systems and CIs to various forms of security challenges. Any form of intrusive action on the SCADA modules and communication networks can create devastating consequences on nations due to their strategic importance to CIs' operations. Therefore, the prompt and efficient detection and classification of SCADA systems intrusions hold great importance for national CIs operational stability. Due to their well-recognized and documented efficiencies, several literature works have proposed numerous supervised learning techniques for SCADA intrusion detection and classification (IDC). This paper presents a critical review of recent studies whereby supervised learning techniques were modelled for SCADA intrusion solutions. The paper aims to contribute to the state-of-the-art, recognize critical open issues and offer ideas for future studies. The intention is to provide a research-based resource for researchers working on industrial control systems security. The analysis and comparison of different supervised learning techniques for SCADA IDC systems were critically reviewed, in terms of the methodologies, datasets and testbeds used, feature engineering and optimization mechanisms and classification procedures. Finally, we briefly summarized some suggestions and recommendations for future research works.

Keywords: artificial neural network; classification; critical infrastructures; industrial control systems; intrusion detection; supervised learning; SCADA; support vector machine

Citation: Alimi, O.A.; Ouahada, K.; Abu-Mahfouz, A.M.; Rimer, S.; Alimi, K.O.A. A Review of Research Works on Supervised Learning Algorithms for SCADA Intrusion Detection and Classification. *Sustainability* **2021**, *13*, 9597. https://doi.org/10.3390/su13179597

Academic Editors: Muhammad Shafiq, Amjad Ali, Farman Ali and Jin-Ghoo Choi

Received: 9 July 2021
Accepted: 31 July 2021
Published: 26 August 2021

1. Introduction

Supervisory Control and Data Acquisition (SCADA) systems play a significant role in providing remote access, monitoring and control of critical infrastructures (CIs), which includes power systems, water distribution systems, gas plants, wastewater collection systems, etc. [1–4]. The stringent real-time requirements, growing interconnectivity, standardization of communication protocols and remote accessibility of modern SCADA systems have contributed massively to the exposure of the infrastructures to various vulnerabilities and security challenges such as sabotage, terrorism and intrusions [5–8]. Historically, when SCADA systems were initially deployed, the goal was to improve CIs' efficiency and effectiveness with little consideration of the potential future security challenges [9,10]. In fact, back in the days, SCADA security issues were majorly due to environmental challenges and equipment failures due to wear and tear. However, advancement in technology in recent years have shifted the focus to varieties of security challenges, which includes cyber intrusions and attacks [11–14]. Proprietary SCADA systems' components which includes the human machine interface (HMI), sensors, master terminal units (MTU), remote terminal

units (RTU), etc. are vulnerable to different forms of intrusions [5,15,16]. Also, the various protocols being used for communication, which include Modbus, DNP3, Profibus, etc., can be remotely targeted, via cyberattacks [4]. Apart from severe operational instabilities, failures, financial losses, etc., SCADA systems vulnerabilities and security challenges can have serious devastating consequences on nations due to their strategic importance to the various CIs [9,17,18]. As explained by the authors in [19,20], documented SCADA systems cyberattacks such as the Stuxnet, Aurora, etc. have shown the grave harms that adversaries can accomplish. The ugly reality is that the attacks and intrusions that target SCADA networks and industrial control systems (ICS) are geometrically increasing in recent times. According to [21], 56% of organizations using SCADA/ICS reported cases of intrusions between the second quarter of 2018 up to the second quarter of 2019. Based on the Trend Micro Zero Day Initiative (ZDI) report [22], Figure 1 depicts a record of the number of discovered SCADA vulnerabilities from the year 2015 to 2019.

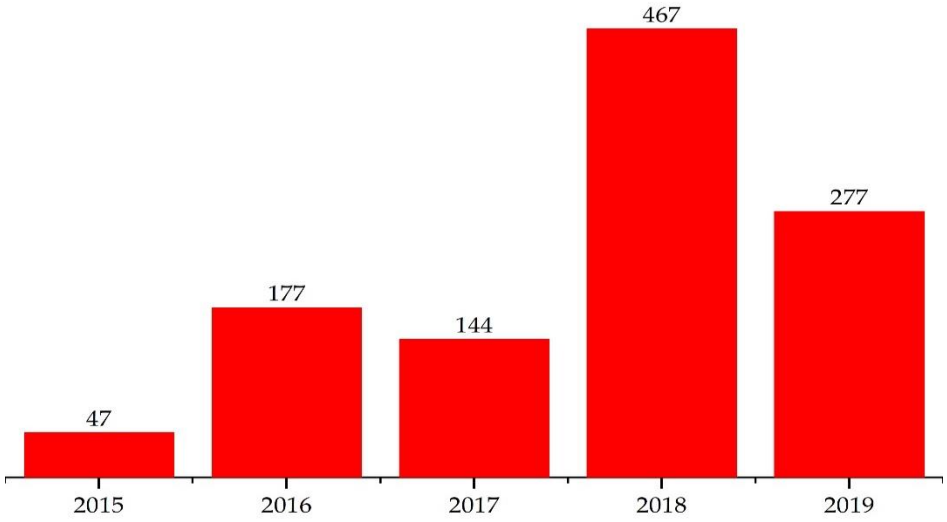

Figure 1. Discovered SCADA vulnerabilities from 2015–2019.

The prompt detection and classification of these SCADA security menaces has consistently been very challenging. With the huge cyber-presence from the various SCADA infrastructures across numerous modern ICS facilities, coupled with the voluminous data generated from the various SCADA sensors and other infrastructure, it is hugely vital to devise modern measures and models that can learn and discover irregular patterns in the SCADA system data and reach meaningful conclusions in the prediction, detection and classification of SCADA intrusions [23].

Historically, most of the proposed security models for traditional SCADA networks were based on statistical formulation theories. However, these models struggle in handling modern SCADA systems due to their complex nature. This limitation calls for better methodologies, such as data driven approaches like machine learning and deep learning methods. The data driven methods have better computing capacity to handle voluminous SCADA datasets, with huge number of features and variables. In fact, SCADA intrusion detection and classification (IDC) is currently one of the most significant areas of machine learning applications. This reflects the increasing number of publications involving machine learning models for SCADA security in recent years. Using a decade gap, and starting from the year 1991, Figure 2 presents an estimate of the number of machine learning-based SCADA security publications, whereby various machine learning models were proposed/deployed for solving and mitigating SCADA security problems including IDC. The publications' statistics in Figure 2 are acknowledged in terms of relevance using [24]. Logically, machine learning algorithms are not the definitive solutions

to all SCADA security menaces. However, they present powerful set of tools that justify thoughtful consideration in dealing with intrusion menaces.

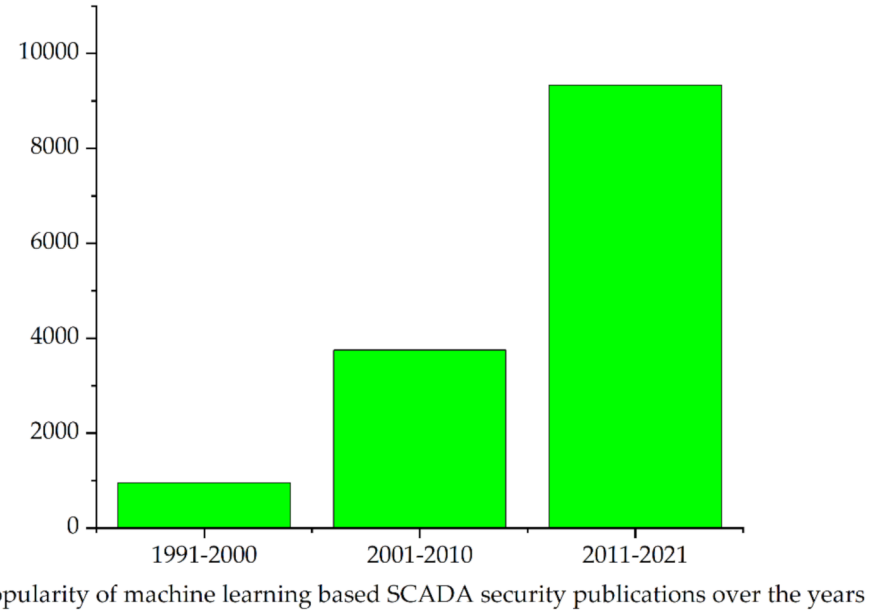

Figure 2. Popularity in machine learning based SCADA security models.

Traditionally, based on the structure and characteristics of datasets, machine learning algorithms are grouped as supervised, semi-supervised and unsupervised learning. Supervised learning algorithms are designed to learn the correlations between features in the training dataset, in order to create a predictive model that has the capacity to infer annotations for another dataset with unknown annotations [23]. On the contrary, unsupervised learning algorithms do not need labelled output. Instead, the goal is to infer some underlying structure that is present within the set of input data points. Semi-supervised learning techniques fall between supervised learning and unsupervised learning [25]. Semi-supervised learning is a type of learning whereby the algorithm is trained upon a combination of labelled and unlabeled datasets.

Supervised learning is arguably the most prominent learning approach for SCADA security tasks. As illustrated in various SCADA security studies in the literature, researchers use the features in the SCADA dataset as training set to infer a model for predicting the annotations of the features in the testing dataset. This paper presents a critical review of recent research works whereby supervised learning algorithms ranging from artificial neural networks (ANN), k-nearest neighbors (k-NN), etc. were modelled for SCADA IDC.

Several articles in the literature has surveyed SCADA security from different viewpoints. Ferrag et al. [26] surveyed SCADA cyber-security challenges and discussed several solutions including data mining solutions. Similarly, Upadhyay [3] reviewed SCADA vulnerabilities and recommendations to strengthen SCADA security. the authors in [27] reviewed SCADA cyber-security risk assessment methodologies. Tariq et al. [1] reviewed cyber threats and defense mechanisms for securing SCADA-based CIs. Rakas et al. [16] focused on network-based solutions for SCADA intrusions. Yaacoub et al. [20] reviewed several security features including vulnerabilities, threats and intrusions. Rezai et al. [10] reviewed key management challenges in SCADA systems. Furthermore, the authors discussed several applications, technologies, standards and communication protocols while identifying and analyzing their limitations. Ahmim et al. [28] also presented a review on intrusion detection systems for SCADA systems. In contrast to other review works in the literature, we critically review, analyze and compare different supervised learning techniques for SCADA IDC, focusing on the methodologies, datasets and testbeds used, feature

engineering and optimization mechanisms and classification procedures. The paper aims to contribute to the state-of-the-art research and recognize critical open issues. We intend to provide a comprehensive summary of research and trends for researchers working in the area of ICS/SCADA security. Finally, we briefly summarized some suggestions and recommendations for future research works.

The rest of the paper is structured as follows. Section 2 briefly describes the methodology adopted for the review. Section 3 presents a brief overview of modern SCADA architecture. In Section 4, we analyze and discuss some prominent supervised learning for SCADA security. In the Section, we analyze the processes of using supervised learning algorithms for SCADA IDC, especially in terms of datasets and testbeds used, feature engineering and optimization mechanisms and classification procedures. In Section 5, we summarized some suggestions and recommendations for future research works. Finally, the last section presents the conclusions.

2. Materials and Methods

In this paper, the authors conduct a comprehensive state-of-the-art review of recent research studies whereby supervised learning techniques were modelled for SCADA IDC. The state-of-the-art research was conducted using popular databases, which include MDPI database, IEEE Explore database, springer database, google scholar database, Wiley online library, ACM digital library, Elsevier database, etc., in order to search for relevant publications. The methodology and criteria used to include a published paper in this work include, but are not limited to, a focus on solving SCADA intrusion detection problem using supervised learning model. For the publication time span, the focus was mainly on recent research works, from the 2018 to 2021. Multiple searches were performed between January 2021 and July 2021. By focusing on recent trends on supervised learning algorithms for SCADA security, the paper intends to provide help to researchers working in the field of ICS security.

3. Brief Overview of Modern SCADA Architecture

Typical modern SCADA system combines hardware components and software programs that operate in a pervasive manner. The components are interconnected using varieties of wired and wireless communication standards. Major architectural components of a modern SCADA system include: field devices, RTUs, MTUs, programmable logic controllers (PLCs), intelligent electronic devices (IEDs), HMI, Historian, etc. [5,16]. Figure 3 presents the simplified architectural structure of a SCADA system. A typical SCADA network collects data from the field devices (sensors, actuators, etc.), which directly engage with the CIs physical equipment such as pumps and valves [29]. The RTUs, PLCs, IEDs assist in retrieving real-time data from the field devices, which control and monitor the actions of the CIs' process [30]. Modern day RTUs, IEDs, etc. are technologically advanced. They send the received data to the MTUs for analysis and processing [3]. Basically, MTUs are the central monitoring station and they assist in the distribution of control commands and data from field devices to control centers. The overall control of the operation is conducted in the control centers, which consist of computers, databases, servers, HMIs, etc. The statuses of the monitored and controlled physical processes are presented on the HMI consoles [2]. Moreover, HMIs present a graphical display of various emergency notifications, such as alerts and warnings, which allow operators to interact with the systems [7,31]. Historians are databases that store the various data gathered by the SCADA systems. The stored data in the historians are used for purposes such as auditing and analysis. As SCADA networks are increasingly adopting certain technologies, vulnerabilities, intrusions and cyberattacks are increasingly becoming major challenges [32,33]. Yadav and Paul [19] explained that, in order to support effective remote access, some of the SCADA nodes are connected to the internet, which exposes them to varieties of network based attacks.

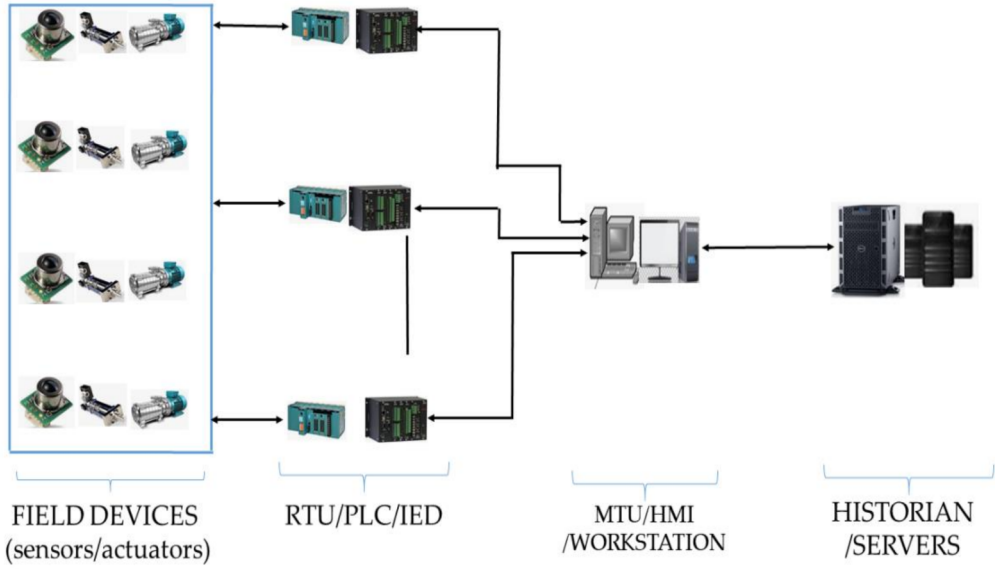

Figure 3. A simplified architecture of a typical SCADA system [5,16,17,34,35].

In recent years, it has become increasingly challenging to protect SCADA systems using traditional methods. As viable alternatives, data mining and analytics methodologies which include machine learning and deep learning models are continuously being proposed as they present exciting advantages, such as high performance, high speed of execution and effectiveness. Generally, data mining and analytics involve the process of learning and identifying patterns or trends in datasets [36].

4. Supervised Learning for SCADA Security

Supervised learning algorithms are aimed at training labelled input data for a particular output [25,37]. The algorithms are trained to detect some underlying patterns between the input dataset and the output labels, which allows them to successfully label unlabeled dataset [31]. Based on the mode of the learning task, supervised learning algorithms are basically categorized into regression and classification. While the output for the regression category takes continuous values and contains an interval on the real line, the output for classification type takes categorical values and they are tagged class labels. Popular supervised learning algorithms include k-NN, ANN, random forest (RF), Bayesian networks (BN), decision tree (DT), etc. Supervised learning algorithms have been consistently and successfully proposed in solving various non-linear problems and fields, such as bioinformatics, handwriting recognition, spam detection, and SCADA IDC. In the literature, various SCADA security researchers have proposed and modelled numerous supervised learning algorithms such as ANN, NB, etc. for SCADA IDC. As explained in [5], data mining and analytics approach for SCADA IDC involves three major processes: Testbed design/dataset generation, feature engineering/preprocessing and prediction/classification/detection.

4.1. Datasets Generation Mechanism Overview

The most important element for the utilization of supervised learning algorithms in SCADA security studies is the deployed dataset/testbed. For the effective application of the various supervised learning algorithms, it is important to have sufficient dataset for the algorithm's training process. Researchers use the features in the SCADA data as training dataset to induce a model for predicting the feature instances in the testing dataset. In the literature, different types of datasets have been deployed in the supervised learning based SCADA security studies. While several authors used various open source datasets such as the popular Knowledge Discovery and Data Mining (KDD99) dataset [38],

UNSW-NB15 dataset [39], iTrust SWAT dataset [40,41], etc., others have modelled different SCADA imitation testbeds using hardware devices and/or software simulators for generating datasets. A detailed review of cyberattack simulation tools was conducted by Nazir et al. [42]. During testbed simulations and dataset generation, diverse attack scenarios are modelled to create well-structured and balanced datasets that mimic real life SCADA intrusion event situations. Some of the popular cyberattacks are denial of service (DoS), false data injections, man-in-the-middle (MITM), etc. [30,43]. To generate a dataset, the authors in [44] and [45] used the popular open source network simulator, Network simulator 2 to model a SCADA system. The authors in [6] used Omnet++ simulator to model a SCADA system. In a related work, Queiroz et al. [46] used SCADASim for building SCADA system. A detailed review of SCADA simulators were done by Mathioudakis et al. [47]. Using a different approach for generating SCADA dataset, the authors in [48] used virtual host Nova and PLC by HoneyD. Similarly, Yang et al. [49] set up several SUN servers and workstations in their security work. The authors in [50] simulated a testbed involving both hardware and software tools which include Allen Bradley PLC controller, Ethernet network, Nmap, Nessus, MetaSploit, etc. to generate SCADA dataset. Branisavljevic et al. [51] used the Belgrade sewage system as testbed to generate SCADA dataset. Yadav [7] presented a detailed review and comparison of several SCADA testbeds developed by various researchers.

Due to the scarce availability of resources among other factors, numerous authors in the literature make use of open source data in their SCADA security studies. The first open source intrusion detection dataset was generated in February 1998 by Defense Advanced Research Project Agency (DARPA), in the MIT Lincoln Laboratory and they initially created the KDD98 dataset [52]. The dataset containing simulated intrusions is made up of network traffic and audit log files. The KDD98 dataset was used for creating the KDD99 dataset. Of all the public datasets used in supervised learning algorithms based SCADA security studies, KDD99 is the most deployed dataset. The dataset was generated from five weeks of experimentation to generate training and testing datasets. Furthermore, the KDD99 attack vectors are categorized as DoS, Probe, Root 2 Local (R2L) and User 2 Root (U2R) [38]. The authors in [48,49,53–55] and several others deployed KDD99 dataset in their SCADA security studies. However, the dataset has been heavily criticized for having a lot of duplicate and redundant records. To improve on some of the KDD99 dataset's limitation, the NSL-KDD dataset was developed by Tavallaee et al. in 2009 [56]. The NSL-KDD dataset does not contain a huge amount of duplicate and redundant packets. Another public dataset, popular among supervised learning algorithm-based SCADA security studies, is the SWAT dataset developed by the iTrust Centre for Research in Cyber Security, Singapore University of Technology and Design (SUTD) [41]. The SWAT testbed framework for the dataset generation is a water distribution system, which is made up of a six-stage process that imitates an actual water treatment facility. For the dataset generation, operation was run for 11 consecutive days, seven days out of the 11 days were run as normal operation while the remaining four days were run under attack scenarios. The authors in [13,57–61] and several others used the SWAT dataset in their research works. Another dataset that is popular within supervised learning algorithms based SCADA security studies is the Mississippi State University (MSU) gas pipeline system SCADA dataset [33]. Table 1 presents a comparison of some popular open source datasets that are commonly deployed in studies involving supervised learning techniques for SCADA IDC.

Table 1. Comparison of commonly deployed open sourced datasets in SCADA security studies [25,39,56,62–72].

Dataset	Published Year	Developer	Brief Description and Comparison: Features and Scenarios	Attacks Type
DARPA (KDD98)	1998	MIT Lincoln Laboratory	Recognized as the earliest open source dataset for intrusion detection studies. It is made up of network traffic and audit log files, which were collected from several internet-linked computers. The training and testing dataset contains seven and two weeks, respectively of network-based attacks in the midst of normal background data.	U2R, R2L, Probing, and DoS attacks
KDD99	1999	University of California	It is an upgraded version of KDD98 dataset. It is made up of approximately 4,900,000 vectors with 41 features, which are categorized into basic, traffic and content features. The dataset generation involves three weeks and two weeks of training and testing respectively. The secondnd week of training data contains several attacks. The testing dataset involves network-based attacks in the midst of normal background data. It has 201 instances of about 56 types of attacks distributed across the testing weeks. The dataset is heavily criticized for having too many duplicate feature instances.	U2R, R2L, Probing, and DoS attacks
NSL-KDD	2009	University of California	The dataset is developed to solve the issues of huge duplicate and redundant packets that is attributed to the KDD99 dataset. As a result of removing duplicate and redundant packets, the dataset contains approximately 150,000 records. The dataset has similar properties and classes as KDD99 dataset i.e it also has 41 features. The training and testing dataset includes 24 and 38 attack types, respectively.	U2R, R2L, Probing, and DoS attacks
UNSW-NB15	2015	Cyber Range Lab of UNSW Canberra, Australia	Unlike previously developed open source datasets, the UNSW-NB15 dataset present a depiction of modern-day network traffic and attack scenarios. The dataset packets were created using tools such as IXIA Perfect-Storm, etc. The dataset contains a variety of normal and attacked activities with class labels of 2,540,044 records with 49 features. The dataset is heavily criticized for having too many duplicates in the training set.	Fuzzers, Analysis, Backdoors, DoS, worm, Exploits, Generic, Reconnaissance, Shellcode.
KYOTO	2006–2009	Kyoto University	The dataset is created using tools, such as honeypots, darknet sensors, e-mail server and web crawler. The dataset has 24 statistical features, whereby 14 features were extracted based on the KDD99 dataset and 10 additional features. The additional 10 features allows effective investigation on the network status.	
CSE-CIC-IDS 2017	2017	Communications Security Establishments (CSE) & the Canadian Institute for Cybersecurity (CIC).	The dataset is an improvement on the earlier developed ISCX2012 dataset. The dataset has the attributes of practical real-world dataset and it is labelled based on the timestamp, source and destination IPs, source and destination ports, protocols and attacks. The dataset has 80 network flow features with 2,830,743 instances, with attack traffic making up approximately 20% of the total number. CICFlowMeter tool is used to extract the 80 features.	Benign behavior, Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet

Table 1. *Cont.*

Dataset	Published Year	Developer	Brief Description and Comparison: Features and Scenarios	Attacks Type
CSE-CIC-IDS 2018	2018	CSE & CIC	The dataset has the same features as the 2017 dataset variant. However, the dataset was modelled using larger network of simulated client targets and attack devices. The attack devices include 50 machines while the victim devices have 420 machines with 30 servers. The dataset involves logs from individual machines, along with 80 features extractions from captured traffic done by CICFlowMeter-V3. The dataset contains 16,233,002 instances with about 17% of the instances being attack traffic.	Brute-force, Heartbleed, Botnet, DoS, DDoS, Web attacks, and infiltration of the network from inside.
SWAT	2016	iTrust Centre for Research in Cyber Security, SUTD	The testbed for the dataset generation is a water distribution system that imitates an actual water treatment facility. For the dataset generation, operation was run for 11 consecutive days, 7 days out of the 11 days were run as normal operation while the remaining 4 days were run under attack scenarios involving 41 attacks.	41 different attacks were simulated during 4 days of attack events.
Morris	Power System-2014, Gas Pipeline-2013, Gas Pipeline & Water-2014 New Gas Pipeline-2015 EMS-2017	Oak Ridge National Laboratories, MSU.	Five datasets were developed: Power system datasets, Gas pipeline datasets, Energy Management System (EMS) dataset, New gas pipeline datasets and Gas pipeline and Water storage tank datasets. The three Power system datasets comprises electric transmission system normal, disturbance, control, cyber-attack behaviors data. The EMS dataset consist of a voluminous anonymized log file that are recorded over 30 days interval. The Gas pipeline, Gas pipeline and water storage tank and New gas pipeline datasets is made up of packets captured from control devices and the HMI in a gas pipeline testbed. The Gas Pipeline and Water Storage Tank datasets has additional packet data captured from a water storage tank.	Some of the attacks include data injection, relay setting change and remote tripping command injection.

4.2. Feature Engineering and Optimization Mechanism

In SCADA security studies involving the use of data mining and analytics methodologies for the prediction, detection and classification of intrusions, the use of feature engineering mechanism for the voluminous dataset(s) is highly important as they have significant impact on the results [4]. The authors in [32] explained that feature engineering tools, such as feature extraction, weighting, selection, reduction, etc. assist in improving the performances of classifiers. Further, considering the problem of imbalanced datasets which is very common with SCADA datasets, feature engineering tools assist in making the classification tasks computationally easier. In the literature, different models and algorithms have been proposed as feature engineering tools in SCADA security studies involving supervised learning algorithms. Waghmare et al. [73] deployed principal component analysis (PCA) for feature reduction for a SCADA dataset. The authors in [74] used PCA, generalized hebbian algorithm, independent component analysis (ICA), singular value decomposition and self-organizing map as feature reduction tool in their SCADA security study. The authors in [75] also used PCA, ICA and canonical correlation analysis for a similar task. In [76], the authors used models based on function code, time factor, etc. as feature extraction tools. In another study, information gain and singular value decomposition was used as feature engineering tools by the authors in [77]. Similarly,

InfoGainAtributeEval, information gain and filter based approach were used as feature engineering tools in [78]. For improved detection and classification, several authors deployed meta-heuristic algorithms such as genetic algorithm (GA), particle swarm optimizer (PSO), etc. as feature engineering and optimization tools. The authors in [32] used GA as feature weighting tool. Similarly, the authors in [59] used GA as feature engineering tool for ANN in classifying SWAT dataset. The authors in [57] used PSO for optimizing the parameters for back-propagation neural network. In related works, the authors in [79,80] used PSO as feature engineering tools in separate security studies involving supervised learning algorithms.

4.3. Classification Mechanism

Various prominent supervised learning algorithms such as SVM, NB, RF, etc. have been proposed in several intrusion prediction, detection and classification of SCADA datasets and other problems that needed to be addressed. In some of the reviewed articles, while some authors proposed singular supervised learning models [32,57], several authors [81–84] ensemble two or more models, with the aim of achieving improved performances. Moreover, some authors compared several supervised learning models on specific dataset(s), in order to establish the best possible model for the analyzed SCADA system and testbed. Additionally, some authors do the comparative study to prove that the individually developed supervised learning model has the capacity to achieve exceptional results within specific context. In this section, some of the widely deployed supervised learning algorithms are discussed.

4.3.1. Support Vector Machine (SVM)

Proposed by Vapnik in the early 90s, SVM is a popular supervised learning method that has consistently been deployed in varieties of classification and regression studies [85]. Most SCADA IDC tasks are binary classification tasks, which makes SVM models suitable for the task. SVMs create an hyperplane, or sets of hyperplanes, in a high-dimensional feature space, which optimally separates the training patterns based on the classes [4,84]. SVMs are robust to high dimensional data and they are well known to have good generalization ability. Even with data that are non-linearly separable in feature space, SVMs has the capacity to perform exceptionally well. Commonly used kernel methods for SVMs are linear, polynomial and sigmoid [32]. The two popular variation of SVMs: one class support vector machines (OCSVM) [86] and support vector data description (SVDD) [87] have been widely proposed by various authors in numerous SCADA security studies. Schuster et al. [88] and Yasakethu et al. [89] deployed OCSVMs in constructing models for the detection of intrusions in a network data. The authors in [90,91] modelled K-Means clustered OCSVM for the classification of SCADA intrusions. Similarly, OCSVM model was also modelled in [92,93] and [51]. Lee et al. [94] developed an OCSVM based detection model with the capacity to learn header-based whitelist and payload and experimented it on a testbed dataset. Maglaras et al. [35] modeled a OCSVM model for detecting cyber-intrusions in a designed small SCADA testbed. Prisco and Duitama [95] also proposed OCSVM for detecting intrusions on SCADA network. In a related work, Fang et al. [96] modelled a support vector regression for predicting a SCADA monitoring data. Terai et al. [97] and Waghmare et al. [73] developed SVM models for detecting intrusions and achieved remarkable results. Wang et al. [85] developed a SVM model for classifying faults in SCADA power system dataset. In a comparative study, the authors in [98] modelled several supervised learning, which include OCSVM, DT, k-NN, etc. for classifying SCADA dataset. From the study, OCSVM presented the best result. In a related work, the authors in [99] did a comparative task using SVM and RF models for classifying two different datasets. Inoue et al. [58] also compared the effectiveness of OCSVM model with deep neural network model in classifying the SWAT dataset. Similarly, the authors in [100] did a comparison work using OCSVM and SVDD models in classifying SCADA system intrusion. For improved classification performance, the author in [101,102] did a hybrid

task involving the ensemble of SVDD and kernel principal component analysis (KPCA) for the classification of SCADA intrusions using the MSU gas pipeline dataset.

4.3.2. Artificial Neural Network (ANN)

ANN is a supervised learning algorithm that is based on the structural framework of the neurons and they have the learning and processing capacity that is similar to a small scale human brain [103]. Similar to SVM, ANNs are quite robust to high dimensional data and they have good generalization ability. The simplest form of ANNs are the perceptrons and they are very useful for the classification of patterns that are linearly separable [84]. In recent years, ANN has been consistently deployed in various SCADA security studies. Shalyga et al. [59] combined GA and ANN for classifying the SWAT SCADA dataset. Neha et al. [104] similarly developed a classification model based on a hybrid salp swarm optimization with ANN. The authors evaluated the developed model using the KDD99 dataset. Also, Demertzis et al. [105] presented an ANN based detection model using 3 SCADA datasets for the evaluation. The authors in [44] used weighted particle based cuckoo search optimization based artificial neural network model for classifying SCADA intrusions. Reuter et al. [31] proposed an artificial neural network based anomaly detection for the CSE-CIC-IDS 2017 dataset. Li et al. [106] modelled a back propagation neural network for analyzing the health assessment for fault and intrusion using wind turbines SCADA dataset. Likewise, Zhang [107] proposed an ANN prediction model with the capacity to generate warning and alarm for wind turbine using a stored SCADA data. With regards to ensemble models, Kosek et al. [108] achieved remarkable results from the ensemble of multiple ANNs for a photovoltaic SCADA dataset. Similarly, Yan et al. [109] developed a multilayer neural network and RF algorithms for detecting intrusions in a wind turbine SCADA dataset.

4.3.3. Decision Tree (DT)

DTs are tree based models. DT is a popular supervised learning method that has consistently been used in varieties of classification and regression studies [110]. Among the popular machine learning models, DT is one of the simplest to understand, visualize and evaluate. As they are non-parametric, outliers do not have much effect on DT models and they also perform reasonably well with linearly inseparable data. Depending on the splitting criteria, popular variation of the DT algorithms include: ID3, C4.5, C5.0 and CART [12]. In recent years, DT has been consistently deployed in various SCADA security studies. McNabb et al. [111] developed a classification model based on DT for predicting intrusions in a SCADA and wide area measurement system dataset. Upadhyay et al. [112] developed a DT classification model for classifying intrusions into power system SCADA network. Mrabet et al. [113] developed a DT based model for detecting intrusive signatures in phase measurement unit dataset. In relation to the ensemble model, Al-Asiri et al. [114] used WEKA to model a couple of DTs in classifying the MSU gas pipeline dataset. Similarly, Siddavatam et al. [115] developed a DT and RF models for detecting intrusions in SCADA traffic. In a comparative study, Swetha and Meena [116] developed a DT, k-NN and SVM models for classifying the KDD99 dataset. From the study, the best results were achieved using DT and SVM. However, it is well-known that DTs struggle in handling high dimensional data as it takes quite a considerable time to build the tree model. Moreover, without proper pruning DTs can easily overfit, a reason several researchers usually opt for the ensemble models of DT, well known as Random Forests.

4.3.4. Random Forest (RF)

Developed by Breiman, RF is an efficient supervised learning algorithm that is widely used in various classification studies [81]. RF is an ensemble method that are constituted by a set of tree structured classifiers. RFs operate by training a couple of DTs and they return the class with the majority over all the trees in the ensemble [109]. Tamy et al. [81] explained that DTs are combinations of sets of tree predictors whereby individual tree depends on

the values of a random vector that is sampled independently with the same distribution for the trees that makes up the forest. Rakhra et al. [110] explained that RFs are collections of multiple DTs whereby the challenge of overfitting which is popular with singular DTs is solved by a voting method, in which the most voted class is the final result for the target observation. Generally, RFs are well-known to be fast, scalable and robust. RFs have been proposed numerously by various authors for SCADA IDC. Alhaidari and AL-Dahasi [83] modelled three supervised learning algorithms: RF, J48 and Naive Bayes for detecting DoS intrusion patterns in SCADA system. Using the KDD99 dataset for the evaluation of the three modelled algorithms, RF presented the best result. Similarly, Choubineh et al. [117] modelled five learners; DT, RF, Naive Bayes, BayesNet and OneR for the classification of gas pipeline SCADA dataset. In the study, the authors deployed cost-sensitive learning with fisher's discriminant analysis to overcome the class imbalance problem. In another related work, the authors in [118] modelled several learners which include RF, SVM, Naive Bayes, OneR, J48, NNge for the detection of intrusions in SCADA network. From the study, RF and NNge presented the best results. Tamy et al. [81] also did a comparative study involving RF, Naïve Bayes, SVM, and J48 Tree using MSU gas pipeline dataset. The authors in [99] also did a comparison work involving two supervised learning algorithms; RF and SVM for the classification of two SCADA datasets. Similarly, Hink et al. [14] successfully explored different learners including RF, SVM, etc. on a SCADA power system dataset.

4.3.5. Bayesian Networks (BN)

BN, otherwise known as belief or bayes network is a probabilistic graphical model that represents variable sets whose conditional probability relationship are represented as a directed acyclic graph with nodes and edges [119,120]. BNs have been explored in varieties of SCADA security studies. Huang et al. [121] proposed a BN model for the security assessment of SCADA network. In a similar study, Shin et al. [122] also modelled BNs for the security evaluation of nuclear SCADA systems. Zhang et al. [123] developed a BN model for evaluating the probability of successful intrusions into SCADA system. In the study, the authors considered six intrusion scenarios which have disturbing effects of tripping circuit breakers. In a related work, the authors in [124] developed two BN models for intrusion procedure illustration and for evaluating the probability of successful intrusions into SCADA network. In the study, the authors considered four intrusion scenarios for the SCADA system cyber-components. Likewise, the scenarios have the effect of tripping circuit breakers. Despite the numerous successes achieved using BN for SCADA security, Borujeni et al. [119] argued that their implementations involve huge computational requirements, especially in fields, such as modern SCADA/ICS systems as there are vast number of nodes involved. BN are known to perform poorly with high dimensional datasets.

4.3.6. K-Nearest Neighbors (k-NN)

k-NN is a distance based supervised learning algorithm which is well known for its simplicity. k-NN's simplicity comes from the fact that it is easy to interpret and its low computation time [125]. Also, they are generally referred to as lazy learners. They use data to classify unforeseen data points by evaluating the distances from the neighbor points [126,127]. They can be deployed for both classification and regression tasks. They are well-suited for multi-modal classes and multi-label applications. In classification and regression tasks, k-NN's performance depend on the choice of the 'k' value. Usually, in different studies, computationally expensive methods such as cross validation are normally used for choosing effective 'k' value. k-NNs have been proposed numerously by various authors for SCADA IDC. Gumaei et al. [128] developed a SCADA intrusion detection model that is based on a k-NN model. In the study, the authors used correlation-based feature selection method as feature reduction technique for the numerous power system SCADA datasets deployed. The authors in [125] modelled five algorithms: k-NN, DT, RF, AdaBoost and Naive Bayes for classifying intrusion into power systems SCADA network.

Similarly, Robles-Durazno et al. [82] modelled k-NN, SVM, DT, ANN and Naive Bayes for detecting intrusions in a simulated water system testbed. The authors realized the testbed using Festo MPA Control Process Rig. From the experimentation, KNN and SVM presented the best results. Also, Phillips et al. [4] modelled a couple of classifiers including k-NN, SVM, DT for detecting anomalous traffic in SCADA systems. Similarly, Arora et al. [127] modelled k-NN, RF, SVM, ANN, DT and Naïve Bayes for detecting intrusions on a SCADA/ICS benchmark dataset. From the study, the best accuracy results were achieved using k-NN and RF.

Table 2 presents the comparison of recently proposed supervised learning based approaches for SCADA systems IDC. Apart from providing key details on the dataset/testbed used, the CI domain and the feature engineering techniques used, Table 2 presents a brief key analysis on the strength and drawbacks from the methodologies. Some of the models proposed in the articles reviewed in Table 2 are developed based on several criteria such as the resources available to the researchers, the specific goal(s) the researchers aims to achieve, etc. Some of these points determine the specific testbed or dataset, choice of methodology procedures, optimization technique(s) deployed, etc. in the research works. Furthermore, the factors that determine the classification and computational performances of the supervised learning algorithms depend on varieties of factors such as the characteristics of the deployed dataset, the pre-processing procedures, the computer and processor specifications, the choice of the learning model(s) parameters, etc. Hence, in different comparative studies involving different supervised learning models (as depicted in Table 2), there are contrasting results' performances from some of the prominent supervised learning models.

Table 2. Comparison of supervised learning based methodologies for SCADA security.

Refs.	Dataset/ Testbed	Protocol	CI Domain	Feature Engineering/Optimization Technique	Algorithm(S) Used	Method Strength /Drawback
[31]	(1) CICIDS2017 (2) IEC dataset	(1) Modbus (2) IEC 60870-5-104	Electric power grid	Synthetic Minority Oversampling Technique	Feed forward neural network	Good result but high false positives from the CICIDS2017 evaluation
[44]	SCADA network simulation using Ns-2 simulator	Modbus		Weighted Particle based Cuckoo Search Optimization	ANN	Accuracy of 95%. Low precision rate when tested on ADFA-LD dataset.
[35]	SCADA testbed simulation	TCP/FIN	Electric power delivery infrastructure	Mapping symbolic-valued attributes to numeric valued attributes and scaling.	OCSVM,	Accuracy of 96.3%. high false alarm and model was not tested on big testbed.
[100]	SDN-based SCADA system simulation	Modbus /TCP	Power systems		OCSVM and SVDD	Approximate accuracy of 98%.
[75]	MSU gas pipeline dataset	Modbus	Gas pipeline	Various techniques Including Bloom filter, PCA, CCA, ICA, and AllKNN.	KNN	Accuracy of 97%. Low detection rate
[99]	MSU gas pipeline dataset	Modbus	Gas pipeline	Gaussian Mixture Model, K-means cluster, Zero imputation and indicators	SVM, RF and Bidirectional Long Short Term Memory	Best results achieved from RF and BLSTM

Table 2. *Cont.*

Refs.	Dataset/ Testbed	Protocol	CI Domain	Feature Engineering/Optimization Technique	Algorithm(S) Used	Method Strength /Drawback
[95]	MSU gas pipeline dataset	Modbus	Gas pipeline		SVDD and KPCA.	Good result achieved.
[57]	SWAT dataset		Water treatment facility	PSO for optimizing the parameters for ANN	Back-propagation neural network	Precision and F1 score of 98.7% & 90.4% respectively.
[13]	SWAT dataset		Water treatment facility	Normalization of all the attributes in the interval between 0 and 1	SVM, ANN, RF, J48, DT, BN, etc.	DT presented the best accuracy with 99.72%, followed closely by RF, SVM, ANN with 99.65%, 98.71% and 98.24% respectively. SVM presented the longest computational time among the models.
[59]	SWAT dataset		Water treatment facility	GA for optimization	ANN	Precision % F1 score of 96.7% and 81.2%.
[83]	KDD99 dataset.				J48, Naive Bayes, RF	DT presented the best result with 99.99% accuracy.
[118]	MSU gas pipeline dataset	Modbus	Gas pipeline		RF, SVM, Naive Bayes, OneR, J48, NNge	RF and NNge presented the best results.
[114]	MSU gas pipeline dataset	Modbus	Gas pipeline		DT	Specific-type accuracy of 98.6%.
[81]	MSU gas pipeline dataset	Modbus	Gas pipeline		Naïve Bayes, SVM, J48 adn RF	RF presented the best accuracy of 99.3% and it took the longest time to build compared to the toher models. It is followed closely by SVM.
[115]	Modelled testbed	Modbus /TCP	Power system		DT and RF	RF presented the better results.
[121]	Modelled chemical reaction process	UDP	Chemical reactor	-	BN	Good performance.

5. Suggestions and Recommendations for Future Works

Despite the numerous successes achieved from the application of several supervised learning algorithms in different SCADA IDC studies, there have been several challenges and open issues that can be considered in future research to improve detections and classifications of intrusions. Considering that SCADA IDC significantly depend on the deployed dataset(s), the current use of publicly available datasets, most of which are obsolete and irrelevant with regards to current and future attack and intrusion trends have continued to show irrelevancy in modern-day SCADA IDC. With the geometric increase in technologically advanced SCADA cyber-intrusions globally, modelling mitigations and

solutions to an outdated problem is inapt. Further, for the current SCADA systems threat environments, the various simulation testbed set ups do not inclusively reflect modern-day network traffic including some of the modelled footprint attacks. Therefore, future research works should focus on realistic modern day SCADA system testbeds with modern-day attack scenarios for experimentation and evaluations. Furthermore, as ensemble methods have shown significant trends in producing effective SCADA IDC results, future researches should dedicate more attention on hybrid intrusion detections and classifications models. Last, a high intrusion detection and classification performances are obviously important. However, if the modelled single or ensemble supervised learning algorithms are computationally complex and they take too much time to detect intrusions, severe damage could have been done on the deployed CIs before the security measures produce results. Therefore, future works should always consider the computational complexities of developed models.

6. Conclusions

Security is a major issue in modern-day SCADA system operations as the networks are constantly under high threats of sophisticated intrusions and attacks. Modern-day SCADA systems security measures are expected to cope with intrusions with adequate and efficient mitigations methods that meet the present and future SCADA security demands. This paper reviewed recent state-of-the-art security research works whereby supervised learning algorithms were implemented for SCADA IDC. Through extensive research and analysis, the paper addressed and compared the methodologies applied in using supervised learning for SCADA systems security in terms of the datasets and testbeds used, feature engineering and optimization mechanisms and classification procedures deployed. Furthermore, open issues and challenges for using supervised-learning techniques for SCADA security are discussed. Some future recommendations for future research works were presented as well.

Author Contributions: Conceptualization, O.A.A., K.O., A.M.A.-M., S.R., and K.O.A.A.; methodology, O.A.A., K.O., A.M.A.-M., S.R., and K.O.A.A.; formal analysis, O.A.A., K.O., A.M.A.-M., and K.O.A.A.; investigation, O.A.A., K.O., A.M.A.-M., and K.O.A.A.; resources O.A.A., K.O. and A.M.A.-M.; data curation, O.A.A., K.O. and A.M.A.-M., writing—original draft preparation, O.A.A., K.O., A.M.A.-M., and K.O.A.A.; writing—review and editing, O.A.A., K.O., A.M.A.-M., S.R., and K.O.A.A.; supervision, K.O. and A.M.A.-M.; project administration, K.O. and A.M.A.-M.; funding acquisition, K.O. and A.M.A.-M. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Council for Scientific and Industrial Research, Pretoria, South Africa, through the SmartNetworks collaboration initiative and IoT-Factory Program (Funded by the Department of Science and Innovation (DSI), South Africa).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Tariq, N.; Asim, M.; Khan, F.A. Securing SCADA-based Critical Infrastructures: Challenges and Open Issues. *Procedia Comput. Sci.* **2019**, *155*, 612–617. [CrossRef]
2. Cifranic, N.; Hallman, R.A.; Romero-Mariona, J.; Souza, B.; Calton, T.; Coca, G. Decepti-SCADA: A cyber deception framework for active defense of networked critical infrastructures. *Internet Things* **2020**, *12*, 100320. [CrossRef]
3. Upadhyay, D.; Sampalli, S. SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Comput. Secur.* **2020**, *89*, 101666. [CrossRef]
4. Phillips, B.; Gamess, E.; Krishnaprasad, S. An evaluation of machine learning-based anomaly detection in a SCADA system using the modbus protocol. In Proceedings of the 2020 ACM Southeast Conference, Tampa, FL, USA, 2–4 April 2020; pp. 188–196.
5. Alimi, A.M.; Ouahada, K.; Abu-Mahfouz, A.M. A Review of Machine Learning Approaches to Power System Security and Stability. *IEEE Access* **2020**, *8*, 113512–113531. [CrossRef]

6. Ahmad, Z.; Durad, M.H. Development of SCADA simulator using omnet. In Proceedings of the 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, 8–12 January 2019; pp. 676–680.
7. Yadav, G.; Paul, K. Architecture and security of SCADA systems: A review. *Int. J. Crit. Infrastruct. Prot.* **2021**, *34*, 100433. [CrossRef]
8. Asghar, M.R.; Hu, Q.; Zeadally, S. Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Comput. Netw.* **2019**, *165*, 106946. [CrossRef]
9. Shlomo, A.; Kalech, M.; Moskovitch, R. Temporal pattern-based malicious activity detection in SCADA systems. *Comput. Secur.* **2021**, *102*, 102153. [CrossRef]
10. Rezai, A.; Keshavarzi, P.; Moravej, Z. Key management issue in SCADA networks: A review. *Eng. Sci. Technol. Int. J.* **2017**, *20*, 354–363. [CrossRef]
11. Yang, Y.; McLaughlin, K.; Sezer, S.; Littler, T.; Im, E.G.; Pranggono, B.; Wang, H.F. Multiattribute SCADA-Specific Intrusion Detection System for Power Networks. *IEEE Trans. Power Deliv.* **2014**, *29*, 1092–1102. [CrossRef]
12. Moon, D.; Im, H.; Kim, I.; Park, J.H. DTB-IDS: An intrusion detection system based on decision tree using behavior analysis for preventing APT attacks. *J. Supercomput.* **2017**, *73*, 2881–2895. [CrossRef]
13. Junejo, K.N.; Goh, J. Behaviour-based attack detection and classification in cyber physical systems using machine learning. In Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security, Xi'an, China, 30 May 2016; pp. 34–43.
14. Hink, R.C.B.; Beaver, J.M.; Buckner, M.A.; Morris, T.; Adhikari, U.; Pan, S. Machine learning for power system disturbance and cyber-attack discrimination. In Proceedings of the 2014 7th International Symposium on Resilient Control Systems (ISRCS), Denver, CO, USA, 19–21 August 2014; pp. 1–8.
15. Miller, B.; Rowe, D. A survey SCADA of and critical infrastructure incidents. In Proceedings of the 1st Annual Conference on Research in Information Technology, Calgary, AB, Canada, 11–13 October 2012; pp. 51–56.
16. Rakas, S.V.B.; Stojanovic, M.D.; Markovic-Petrovic, J.D. A Review of Research Work on Network-Based SCADA Intrusion Detection Systems. *IEEE Access* **2020**, *8*, 93083–93108. [CrossRef]
17. el Kalam, A.A. Securing SCADA and critical industrial systems: From needs to security mechanisms. *Int. J. Crit. Infrastruct. Prot.* **2021**, *32*, 100394. [CrossRef]
18. Kabore, R.; Kouassi, A.; N'Goran, R.; Asseu, O.; Kermarrec, Y.; Lenca, P. Review of Anomaly Detection Systems in Industrial Control Systems Using Deep Feature Learning Approach. *Enginerring* **2021**, *13*, 30–44. [CrossRef]
19. Yadav, G.; Paul, K. Assessment of SCADA System Vulnerabilities. In Proceedings of the 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Zaragoza, Spain, 10–13 September 2019; pp. 1737–1744.
20. Yaacoub, J.-P.A.; Salman, O.; Noura, H.N.; Kaaniche, N.; Chehab, A.; Malli, M. Cyber-physical systems security: Limitations, issues and future trends. *Microprocess. Microsyst.* **2020**, *77*, 103201. [CrossRef]
21. Fortinet, Independent Study on SCADA/ICS Security Risks. Available online: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/WP-Independent-Study-Pinpoints-Significant-Scada-ICS-Cybersecurity-Risks.pdf (accessed on 19 May 2021).
22. Trend Micro Zero Day Initiative. Available online: https://www.trendmicro.com/en_no/about/newsroom/press-releases/2019/2019-12-03-trend-micros-zero-day-initiative-leads-vulnerability-disclosure-landscape-in-independent-research.html (accessed on 22 May 2021).
23. Ahmed, M.; Anwar, A.; Mahmood, A.N.; Shah, Z.; Maher, M.J. An Investigation of Performance Analysis of Anomaly Detection Techniques for Big Data in SCADA Systems. *EAI Endorsed Trans. Ind. Netw. Intell. Syst.* **2015**, *2*, 5. [CrossRef]
24. Microsoft Academic. Available online: https://academic.microsoft.com/ (accessed on 26 June 2021).
25. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity* **2019**, *2*, 20. [CrossRef]
26. Ferrag, M.A.; Babaghayou, M.; Yazici, M.A. Cyber security for fog-based smart grid SCADA systems: Solutions and challenges. *J. Inf. Secur. Appl.* **2020**, *52*, 102500. [CrossRef]
27. Cherdantseva, Y.; Burnap, P.; Blyth, A.; Eden, P.; Jones, K.; Soulsby, H.; Stoddart, K. A review of cyber security risk assessment methods for SCADA systems. *Comput. Secur.* **2016**, *56*, 1–27. [CrossRef]
28. Ahmim, A.; Ferrag, M.A.; Maglaras, L.; Derdour, M.; Janicke, H.; Drivas, G. Taxonomy of Supervised Machine Learning for Intrusion Detection Systems. *Sustain. Transp. Dev. Innov. Technol.* **2020**, 619–628. [CrossRef]
29. Samdarshi, R.; Sinha, N.; Tripathi, P. A triple layer intrusion detection system for SCADA security of electric utility. In Proceedings of the 2015 Annual IEEE India Conference (INDICON), New Delhi, India, 17–20 December 2015; pp. 1–5.
30. Alimi, A.M.; Ouahada, K. Security Assessment of the Smart Grid: A Review focusing on the NAN Architecture. In Proceedings of the 2018 IEEE 7th International Conference on Adaptive Science & Technology (ICAST), Accra, Ghana, 22–24 August 2018; pp. 1–8.
31. Reuter, L.; Jung, O.; Magin, J. Neural network based anomaly detection for SCADA systems. In Proceedings of the 2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), Paris, France, 24–27 February 2020; pp. 194–201.
32. Alimi, O.A.; Ouahada, K.; Abu-Mahfouz, A.M.; Rimer, S. Power system events classification using genetic algorithm based feature weighting technique for support vector machine. *Heliyon* **2021**, *7*, e05936. [CrossRef]

33. Paramkusem, K.M.; Aygun, R.S. Classifying Categories of SCADA Attacks in a Big Data Framework. *Ann. Data Sci.* **2018**, *5*, 359–386. [CrossRef]
34. Zhu, B.; Joseph, A.D.; Sastry, S. A Taxonomy of Cyber Attacks on SCADA Systems. In Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, Dalian, Liaoning, China, 19–22 October 2011; pp. 380–388.
35. Maglaras, L.A.; Jiang, J.; Cruz, T.J. Combining ensemble methods and social network metrics for improving accuracy of OCSVM on intrusion detection in SCADA systems. *J. Inf. Secur. Appl.* **2016**, *30*, 15–26. [CrossRef]
36. Ranganathan, G.; Rocha, A. Inventive Communication and Computational Technologies. In Proceedings of the 4th International Conference on Inventive Communication and Computational Technologies (ICICCT 2020), Tamil Nadu, India, 28–29 May 2020.
37. Shakarami, A.; Ghobaei-Arani, M.; Shahidinejad, A. A survey on the computation offloading approaches in mobile edge computing: A machine learning-based perspective. *Comput. Netw.* **2020**, *182*, 107496. [CrossRef]
38. Özgür, A.; Erdem, H. A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015. *PeerJ Prepr.* **2016**, *4*, e1954v1.
39. Moustafa, N.; Slay, J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, ACT, Australia, 10–12 November 2015; pp. 1–6.
40. Goh, J.; Adepu, S.; Junejo, K.N.; Mathur, A. A Dataset to Support Research in the Design of Secure Water Treatment Systems. In Proceedings of the International Conference on Critical Information Infrastructures Security, Paris, France, 10–12 October 2016; pp. 88–99.
41. Singapore University of Technology and Design. iTrust, Centre for Research in Cyber Security. Available online: https://itrust.sutd.edu.sg/itrust-labs-home/itrust-labs_swat (accessed on 15 July 2021).
42. Nazir, S.; Patel, S.; Patel, D. Assessing and augmenting SCADA cyber security: A survey of techniques. *Comput. Secur.* **2017**, *70*, 436–454. [CrossRef]
43. Alimi, K.O.A.; Ouahada, K.; Abu-Mahfouz, A.M.; Rimer, S. A Survey on the Security of Low Power Wide Area Networks: Threats, Challenges, and Potential Solutions. *Sensors* **2020**, *20*, 5800. [CrossRef]
44. Shitharth, S. An enhanced optimization based algorithm for intrusion detection in SCADA network. *Comput. Secur.* **2017**, *70*, 16–26. [CrossRef]
45. Wang, C.; Fang, L.; Dai, Y. A Simulation Environment for SCADA Security Analysis and Assessment. In Proceedings of the 2010 International Conference on Measuring Technology and Mechatronics Automation, Changsha, China, 13–14 March 2010; pp. 342–347.
46. Queiroz, C.; Mahmood, A.; Tari, Z. SCADASim—A Framework for Building SCADA Simulations. *IEEE Trans. Smart Grid* **2011**, *2*, 589–597. [CrossRef]
47. Mathioudakis, K.; Frangiadakis, N.; Merentitis, A.; Gazis, V. Towards generic SCADA simulators: A survey of existing multi-purpose co-simulation platforms, best practices and use-cases. *AGT Group (R D) GmbH Hilpertstrasse* **2013**, *35*, 64295.
48. Gao, J.; Gan, L.; Buschendorf, F.; Zhang, L.; Liu, H.; Li, P.; Dong, X.; Lu, T. Omni SCADA Intrusion Detection Using Deep Learning Algorithms. *IEEE Internet Things J.* **2021**, *8*, 951–961. [CrossRef]
49. Yang, D.; Usynin, A.; Hines, J.W. Anomaly-based intrusion detection for SCADA systems. In Proceedings of the 5th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies (Npic&hmit 05), Knoxville, TN, USA, 12–16 November 2006; pp. 12–16.
50. Linda, O.; Vollmer, T.; Manic, M. Neural Network based Intrusion Detection System for critical infrastructures. In Proceedings of the 2009 International Joint Conference on Neural Networks, Atlanta, GA, USA, 14–19 June 2009; pp. 1827–1834.
51. Branisavljević, N.; Kapelan, Z.; Prodanovic, D. Improved real-time data anomaly detection using context classification. *J. Hydroinform.* **2011**, *13*, 307–323. [CrossRef]
52. MIT Lincoln Laboratory. 1998 Darpa Intrusion Detection Evaluation Dataset. Available online: https://www.ll.mit.edu/r-d/datasets/1998-darpa-intrusion-detection-evaluation-dataset (accessed on 26 July 2021).
53. Zhang, Y.; Wang, L.; Sun, W.; Ii, R.C.G.; Alam, M. Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids. *IEEE Trans. Smart Grid* **2011**, *2*, 796–808. [CrossRef]
54. Poojitha, G.; Kumar, K.N.; Reddy, P.J. Intrusion Detection using Artificial Neural Network. In Proceedings of the 2010 Second International Conference on Computing, Communication and Networking Technologies, Karur, India, 29–31 July 2010; pp. 1–7.
55. Al-Daweri, M.S.; Abdullah, S.; Ariffin, K.A.Z. A homogeneous ensemble based dynamic artificial neural network for solving the intrusion detection problem. *Int. J. Crit. Infrastruct. Prot.* **2021**, *34*, 100449. [CrossRef]
56. Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 8–10 July 2009; pp. 1–6.
57. Alimi, O.A.; Ouahada, K.; Abu-Mahfouz, A.M.; Rimer, S.; Adefemi Alimi, K.O. Intrusion Detection for Water Distribution Systems based on an Hybrid Particle Swarm Optimization with Back Propagation Neural Network. *IEEE Africon* **2021**, accepted.
58. Inoue, J.; Yamagata, Y.; Chen, Y.; Poskitt, C.; Sun, J. Anomaly Detection for a Water Treatment System Using Unsupervised Machine Learning. In Proceedings of the 2017 IEEE International Conference on Data Mining Workshops (ICDMW), New Orleans, LA, USA, 18–21 November 2017; pp. 1058–1065.

59. Shalyga, D.; Filonov, P.; Lavrentyev, A. Anomaly detection for water treatment system based on neural network with automatic architecture optimization. *arXiv* **2018**, arXiv:1807.07282.
60. Zizzo, G.; Hankin, C.; Maffeis, S.; Jones, K. Intrusion detection for industrial control systems: Evaluation analysis and adversarial attacks. *arXiv* **2019**, arXiv:1911.04278.
61. Li, D.; Chen, D.; Jin, B.; Shi, L.; Goh, J.; Ng, S.-K. MAD-GAN: Multivariate Anomaly Detection for Time Series Data with Generative Adversarial Networks. In *Lecture Notes in Computer Science*; Springer Science and Business Media LLC: Berlin/Heidelberg, Germany, 2019; pp. 703–716.
62. Ferrag, M.A.; Maglaras, L.; Moschoyiannis, S.; Janicke, H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *J. Inf. Secur. Appl.* **2020**, *50*, 102419. [CrossRef]
63. Choi, S.; Yun, J.-H.; Kim, S.-K. A Comparison of ICS Datasets for Security Research Based on Attack Paths. In Proceedings of the International Conference on Critical Information Infrastructures Security, Kaunas, Lithuania, 24–26 September 2018; pp. 154–166.
64. Sharafaldin, I.; Lashkari, A.H.; Ghorbani, A.A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. In Proceedings of the ICISSP 2018, Madeira, Portugal, 22–24 January 2018; pp. 108–116.
65. Lin, Q.; Verwer, S.; Kooij, R.; Mathur, A. Using Datasets from Industrial Control Systems for Cyber Security Research and Education. In Proceedings of the International Conference on Critical Information Infrastructures Security, Linköping, Sweden, 23–25 September 2019; pp. 122–133.
66. Conti, M.; Donadel, D.; Turrin, F. A Survey on Industrial Control System Testbeds and Datasets for Security Research. *arXiv* **2021**, arXiv:2102.05631.
67. Kilincer, I.F.; Ertam, F.; Sengur, A. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Comput. Netw.* **2021**, *188*, 107840. [CrossRef]
68. Choudhary, S.; Kesswani, N. Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT. *Procedia Comput. Sci.* **2020**, *167*, 1561–1573. [CrossRef]
69. Sonule, A.R.; Kalla, M.; Jain, A.; Chouhan, D.S. UNSWNB15 Dataset and Machine Learning Based Intrusion Detection Systems. *Int. J. Eng. Adv. Technol.* **2020**, *9*, 2638–2648.
70. Song, J.; Takakura, H.; Okabe, Y. Description of Kyoto University Benchmark Data. Available online: http://Www.Takakura.Com/Kyoto_data/BenchmarkData-Description-V5.Pdf (accessed on 26 June 2021).
71. Suman, C.; Tripathy, S.; Saha, S. Building an effective intrusion detection system using unsupervised feature selection in multi-objective optimization framework. *arXiv* **2019**, arXiv:1905.06562.
72. Kim, J.; Kim, J.; Kim, H.; Shim, M.; Choi, E. CNN-Based Network Intrusion Detection against Denial-of-Service Attacks. *Electronics* **2020**, *9*, 916. [CrossRef]
73. Waghmare, S.; Kazi, F.; Singh, N. Data driven approach to attack detection in a cyber-physical smart grid system. In Proceedings of the 2017 Indian Control Conference (ICC), Guwahati, India, 4–6 January 2017; pp. 271–276.
74. Mansouri, A.; Majidi, B.; Shamisa, A. Anomaly detection in industrial control systems using evolutionary-based optimization of neural networks. *Commun. Adv. Comput. Sci. Appl.* **2017**, *2017*, 49–55. [CrossRef]
75. Khan, I.A.; Pi, D.; Khan, Z.U.; Hussain, Y.; Nawaz, A. HML-IDS: A Hybrid-Multilevel Anomaly Prediction Approach for Intrusion Detection in SCADA Systems. *IEEE Access* **2019**, *7*, 89507–89521. [CrossRef]
76. Kalech, M. Cyber-attack detection in SCADA systems using temporal pattern recognition techniques. *Comput. Secur.* **2019**, *84*, 225–238. [CrossRef]
77. Wang, H.; Lu, T.; Dong, X.; Li, P.; Xie, M. Hierarchical Online Intrusion Detection for SCADA Networks. *arXiv* **2016**, arXiv:1611.09418, 2016.
78. Ullah, I.; Mahmoud, Q.H. A hybrid model for anomaly-based intrusion detection in SCADA networks. In Proceedings of the 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 11–14 December 2017; pp. 2160–2167.
79. Ali, M.H.; Fadlizolkipi, M.; Firdaus, A.; Khidzir, N.Z. A hybrid Particle swarm optimization -Extreme Learning Machine approach for Intrusion Detection System. In Proceedings of the 2018 IEEE Student Conference on Research and Development (SCOReD), Bangi, Selangor, Malaysia, 26–28 November 2018; pp. 1–4.
80. Shang, W.; Zeng, P.; Wan, M.; Li, L.; An, P. Intrusion detection algorithm based on OCSVM in industrial control system. *Secur. Commun. Netw.* **2015**, *9*, 1040–1049. [CrossRef]
81. Tamy, S.; Belhadaoui, H.; Rabbah, M.A.; Rabbah, N.; Rifi, M. An Evaluation of Machine Learning Algorithms to Detect Attacks in Scada Network. In Proceedings of the 7th Mediterranean Congress of Telecommunications (CMT), Fes, Morocco, 24–25 October 2019; pp. 1–5.
82. Robles-Durazno, A.; Moradpoor, N.; McWhinnie, J.; Russell, G. Real-time anomaly intrusion detection for a clean water supply system, utilising machine learning with novel energy-based features. In Proceedings of the 2020 International Joint Conference on Neural Networks (IJCNN), Glasgow, UK, 19–24 July 2020; pp. 1–8.
83. Alhaidari, F.A.; Al-Dahasi, E.M. New Approach to Determine DDoS Attack Patterns on SCADA System Using Machine Learning. In Proceedings of the 2019 International Conference on Computer and Information Sciences (ICCIS), Aljouf, Saudi Arabia, 10–11 April 2019; pp. 1–6.
84. Alimi, A.M.; Ouahada, K.; Abu-Mahfouz, A.M. Real Time Security Assessment of the Power System Using a Hybrid Support Vector Machine and Multilayer Perceptron Neural Network Algorithms. *Sustainability* **2019**, *11*, 3586. [CrossRef]

85. Wang, Y.; Wu, C.; Wan, L.; Liang, Y. A study on SVM with feature selection for fault diagnosis of power systems. In Proceedings of the 2010 The 2nd International Conference on Computer and Automation Engineering (ICCAE), Singapore, 26–28 February 2010; Volume 2, pp. 173–176.
86. Alam, S.; Sonbhadra, S.K.; Agarwal, S.; Nagabhushan, P. One-class support vector classifiers: A survey. *Knowl. Based Syst.* **2020**, *196*, 105754. [CrossRef]
87. Turkoz, M.; Kim, S.; Son, Y.; Jeong, M.K.; Elsayed, E.A. Generalized support vector data description for anomaly detection. *Pattern Recognit.* **2020**, *100*, 107119. [CrossRef]
88. Schuster, F.; Paul, A.; Rietz, R.; Koenig, H. Potentials of Using One-Class SVM for Detecting Protocol-Specific Anomalies in Industrial Networks. In Proceedings of the 2015 IEEE Symposium Series on Computational Intelligence, Cape Town, South Africa, 7–10 December 2015; pp. 83–90.
89. Yasakethu, S.L.P.; Jiang, J.; Graziano, A. Intelligent risk detection and analysis tools for critical infrastructure protection. *Eurocon* **2013**, 52–59. [CrossRef]
90. Jiang, J.; Yasakethu, L. Anomaly Detection via One Class SVM for Protection of SCADA Systems. In Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Beijing, China, 10–12 October 2013; Volume 10–12, pp. 82–88.
91. Maglaras, L.A.; Jiang, J. OCSVM model combined with K-means recursive clustering for intrusion detection in SCADA systems. In Proceedings of the 10th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, Rhodes, Greece, 18–20 August 2014; pp. 133–134.
92. Maglaras, L.; Jiang, J. Intrusion detection in SCADA systems using machine learning techniques. In Proceedings of the Science and Information Conference, London, UK, 27–29 August 2014; pp. 626–631.
93. Cruz, T.; Rosa, L.; Proenca, J.; Maglaras, L.; Aubigny, M.; Lev, L.; Jiang, J.; Simoes, P. A Cybersecurity Detection Framework for Supervisory Control and Data Acquisition Systems. *IEEE Trans. Ind. Inform.* **2016**, *12*, 2236–2246. [CrossRef]
94. Lee, S.; Lee, S.; Yoo, H.; Kwon, S.; Shon, T. Design and implementation of cybersecurity testbed for industrial IoT systems. *J. Supercomput.* **2018**, *74*, 4506–4520. [CrossRef]
95. Prisco, A.F.S.; Duitama, M.J.F. Intrusion detection system for SCADA platforms through machine learning algorithms. In Proceedings of the 2017 IEEE Colombian Conference on Communications and Computing (COLCOM), Cartagena, Colombia, 16–18 August 2017; pp. 1–6.
96. Fang, R.; Wang, Y.; Shang, R.; Liang, Y.; Wang, L.; Peng, C. The ultra-short term power prediction of wind farm considering operational condition of wind turbines. *Int. J. Hydrogen Energy* **2016**, *41*, 15733–15739. [CrossRef]
97. Terai, A.; Abe, S.; Kojima, S.; Takano, Y.; Koshijima, I. Cyber-Attack Detection for Industrial Control System Monitoring with Support Vector Machine Based on Communication Profile. In Proceedings of the 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS & PW), Paris, France, 26–28 April 2017; pp. 132–138.
98. Qu, H.; Qin, J.; Liu, W.; Chen, H. Instruction Detection in SCADA/Modbus Network Based on Machine Learning. In Proceedings of the International Conference on Machine Learning and Intelligent Communications, Weihai, China, 5–6 August 2017; pp. 437–454.
99. Perez, R.L.; Adamsky, F.; Soua, R.; Engel, T. Machine Learning for Reliable Network Attack Detection in SCADA Systems. In Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, New York, NY, USA; 2018; pp. 633–638.
100. Da Silva, E.G.; Da Silva, A.S.; Wickboldt, J.; Smith, P.; Granville, L.Z.; Filho, A.E.S. A One-Class NIDS for SDN-Based SCADA Systems. In Proceedings of the 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, USA, 10–14 June 2016; Volume 1, pp. 303–312.
101. Beauseroy, P.; Honeine, P.; Nader, P. Intrusion Detection in Scada Systems Using One-Class Classification. In Proceedings of the 21st European Signal Processing Conference (EUSIPCO 2013), Marrakech, Morocco, 9–13 September 2013; pp. 9–13.
102. Nader, P.; Honeine, P.; Beauseroy, P. l_p-norms in One-Class Classification for Intrusion Detection in SCADA Systems. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2308–2317. [CrossRef]
103. Boonprong, S.; Cao, C.; Chen, W.; Ni, X.; Xu, M.; Acharya, B.K. The Classification of Noise-Afflicted Remotely Sensed Data Using Three Machine-Learning Techniques: Effect of Different Levels and Types of Noise on Accuracy. *ISPRS Int. J. Geo-Inf.* **2018**, *7*, 274. [CrossRef]
104. Neha, N.; Raman, M.R.G.; Somu, N.; Senthilnathan, R.; Sriram, V.S. An Improved Feedforward Neural Network Using Salp Swarm Optimization Technique for the Design of Intrusion Detection System for Computer Network. In *Advances in Intelligent Systems and Computing*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 867–875.
105. Demertzis, K.; Iliadis, L.; Spartalis, S. A Spiking One-Class Anomaly Detection Framework for Cyber-Security on Industrial Control Systems. In Proceedings of the International Conference on Engineering Applications of Neural Networks, Athens, Greece, 25–27 August 2017; pp. 122–134.
106. Li, H.; Yang, J.; Zhang, M.; Guo, S.; Lv, W.; Liu, Z.; Hui, L. A method based on artificial neural network to estimate the health of wind turbine. In Proceedings of the 27th Chinese Control and Decision Conference (2015 CCDC), Qingdao, China, 23–25 May 2015; pp. 919–922.
107. Zhang, Z. Automatic Fault Prediction of Wind Turbine Main Bearing Based on SCADA Data and Artificial Neural Network. *Open J. Appl. Sci.* **2018**, *8*, 211–225. [CrossRef]

108. Kosek, A.M.; Gehrke, O. Ensemble regression model-based anomaly detection for cyber-physical intrusion detection in smart grids. In Proceedings of the 2016 IEEE Electrical Power and Energy Conference (EPEC), Ottawa, ON, Canada, 12–14 October 2016; pp. 1–7.
109. Yan, X.; Jin, Y.; Xu, Y.; Li, R. Wind Turbine Generator Fault Detection Based on Multi-Layer Neural Network and Random Forest Algorithm. In Proceedings of the IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia), Chengdu, China, 21–24 May 2019; pp. 4132–4136.
110. Rakhra, M.; Soniya, P.; Tanwar, D.; Singh, P.; Bordoloi, D.; Agarwal, P.; Takkar, S.; Jairath, K.; Verma, N. Crop Price Prediction Using Random Forest and Decision Tree Regression: A review. *Mater. Today Proc.* **2021**, in press.
111. McNabb, P.; Wilson, D.; Bialek, J. Classification of mode damping and amplitude in power systems using synchrophasor measurements and classification trees. *IEEE Trans. Power Syst.* **2013**, *28*, 1988–1996. [CrossRef]
112. Upadhyay, D.; Manero, J.; Zaman, M.; Sampalli, S. Gradient Boosting Feature Selection with Machine Learning Classifiers for Intrusion Detection on Power Grids. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 1104–1116. [CrossRef]
113. El Mrabet, Z.; Selvaraj, D.F.; Ranganathan, P. Adaptive Hoeffding Tree with Transfer Learning for Streaming Synchrophasor Data Sets. In Proceedings of the 2019 IEEE International Conference on Big Data, Los Angeles, CA, USA, 9–12 December 2019; pp. 5697–5704.
114. Al-Asiri, M.; El-Alfy, E.-S.M. On Using Physical Based Intrusion Detection in SCADA Systems. *Procedia Comput. Sci.* **2020**, *170*, 34–42. [CrossRef]
115. A Siddavatam, I.; Satish, S.; Mahesh, W.; Kazi, F. An ensemble learning for anomaly identification in SCADA system. In Proceedings of the 7th International Conference on Power Systems (ICPS), Pune, India, 21–23 December 2017; pp. 457–462.
116. Swetha, R.B.S.; Meena, K.G. Smart grid-A network-based intrusion detection system. *Int. J. Comput. Appl.* **2015**, *975*, 8887.
117. Choubineh, A.; Wood, D.A.; Choubineh, Z. 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. *Int. J. Crit. Infrastruct. Prot.* **2020**, *29*, 100357. [CrossRef]
118. Beaver, J.M.; Hink, R.B.; Buckner, M. An Evaluation of Machine Learning Methods to Detect Malicious SCADA Communications. In Proceedings of the 2013 12th International Conference on Machine Learning and Applications, Miami, FL, USA, 4–7 December 2013; Volume 2, pp. 54–59.
119. Borujeni, S.E.; Nannapaneni, S.; Nguyen, N.H.; Behrman, E.C.; Steck, J.E. Quantum circuit representation of Bayesian networks. *Expert Syst. Appl.* **2021**, *176*, 114768. [CrossRef]
120. Friedman, N.; Geiger, D.; Goldszmidt, M. Bayesian Network Classifiers. *Mach. Learn.* **1997**, *29*, 131–163. [CrossRef]
121. Huang, K.; Zhou, C.; Tian, Y.-C.; Tu, W.; Peng, Y. Application of Bayesian network to data-driven cyber-security risk assessment in SCADA networks. In Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, Australia, 22–24 November 2017; pp. 1–6.
122. Shin, J.; Son, H.; Heo, G. Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET. *Nucl. Eng. Technol.* **2017**, *49*, 517–524. [CrossRef]
123. Zhang, Y.; Xiang, Y.; Wang, L. Reliability analysis of power grids with cyber vulnerability in SCADA system. In Proceedings of the 2014 IEEE PES General Meeting Conference & Exposition, National Harbor, MD, USA, 27–31 July 2014; pp. 1–5.
124. Zhang, Y.; Wang, L.; Xiang, Y.; Ten, C.-W. Power System Reliability Evaluation with SCADA Cybersecurity Considerations. *IEEE Trans. Smart Grid* **2015**, *6*, 1707–1721. [CrossRef]
125. Alimi, O.A.; Ouahada, K.; Abu-Mahfouz, A.M.; Alimi, K.O.A. Empirical Comparison of Machine Learning Algorithms for Mitigating Power Systems Intrusion Attacks. In Proceedings of the 2020 International Symposium on Networks, Computers and Communications (ISNCC), Montreal, QC, Canada, 20–22 October 2020; pp. 1–5.
126. Mokhtari, S.; Abbaspour, A.; Yen, K.; Sargolzaei, A. A Machine Learning Approach for Anomaly Detection in Industrial Control Systems Based on Measurement Data. *Electronics* **2021**, *10*, 407. [CrossRef]
127. Arora, P.; Kaur, B.; Teixeira, M.A. Evaluation of Machine Learning Algorithms Used on Attacks Detection in Industrial Control Systems. *J. Inst. Eng. Ser. B* **2021**, *102*, 605–616. [CrossRef]
128. Gumaei, A.; Hassan, M.M.; Huda, S.; Hassan, R.; Camacho, D.; Del Ser, J.; Fortino, G. A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids. *Appl. Soft Comput.* **2020**, *96*, 106658. [CrossRef]