IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 3 July 2023, accepted 19 July 2023, date of publication 26 July 2023, date of current version 2 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3299208

SURVEY

A Review on Data-Driven Security Assessment of Power Systems: Trends and Applications of Artificial Intelligence

ALIREZA MEHRZAD[1], MILAD DARMIANI[1], YASHAR MOUSAVI[2], (Member, IEEE), MIADREZA SHAFIE-KHAH[3], (Senior Member, IEEE), AND MOHAMMADREZA AGHAMOHAMMADI[4]

[1]Department of Electrical Engineering, University of Birjand, Birjand 9717434765, Iran
[2]Department of Applied Science, School of Computing, Engineering and Built Environment, Glasgow Caledonian University, G4 0BA Glasgow, U.K.
[3]School of Technology and Innovations, University of Vaasa, 65200 Vaasa, Finland
[4]Electrical Engineering Faculty, Shahid Beheshti University 1983969411, Tehran, Iran

Corresponding author: Miadreza Shafie-Khah (mshafiek@uwasa.fi)

ABSTRACT Boosting the complexity of the electricity network, penetration of renewable resources, and modernization of power systems has resulted in an increase in the complexity of the power systems security assessment (PSSA). In this context, to decrease the vulnerability of the systems to multiple instability threats and security issues while ensuring the safe operation of the power systems, providing effective online security assessment methods capable of monitoring the systems' security under varying conditions is vital. However, although the traditional methods have demonstrated efficient PSSA performance, intelligent data-driven approaches have effectively overcome the traditional approaches by delivering impressive and rapid PSSA performance. Artificial intelligence (AI) -based techniques are required to guarantee the efficient, optimal, and safe security assessment. The usage of AI is emphasized due to its computational speed for online performance and its flexibility for providing corrective actions for insecure operating conditions to achieve a seamless transition in power systems. In this review, various available data-driven methods in power system security are comprehensively reviewed into two primary classifications: static and dynamic security assessment. The evaluated study aims to highlight the merits and demerits of developed techniques as well as their limitations to provide decision-making assistant for future investigations.

INDEX TERMS Power systems security assessment, data-driven, artificial intelligence, machine learning.

ABBREVIATIONS

AANN	Artificial adaptive neural network.
AEP	American electric power.
ANFIS	Adaptive neuro-fuzzy inference system.
ANN	Artificial neural network.
CART	Classification and regression trees.
CNN	Convolutional neural network.
CVM	Core vector machine.
DA	Data acquisition.
DE	Differential evolution.
DG	Distributed generation.
DL	Deep learning.
DSA	Dynamic security assessment.
DT	Decision tree.
EML	Extreme machine learning.
FIS	Fuzzy inference system.
GA	Genetic algorithm.
GAN	Generative adversarial network.
IoT	Internet of things.
IRF	Iterated random forest.
MFNN	Multi-layer feed-forward neural network.
MLP	Multilayer perceptron.
PD	Pattern discovery.
PMI	Partial mutual information.
PMU	Phasor measurement unit.
PNN	Probabilistic neural networks

The associate editor coordinating the review of this manuscript and approving it for publication was Yu-Huei Cheng.

PSO	Particle swarm optimization.
PSSA	Power system security assessment.
RBFNN	Radial basis function neural network.
ROCOF	Rate of change of frequency.
RVFLN	Random vector functional link network.
SDAE	Stacked denoising auto encoder.
SFS	Sequential forward selection.
SSA	Static security assessment.
SVM	Support vector machine.
TEF	Transient energy function.
TL	Transfer learning.
TSA	Transient stability analysis.
WAMS	Wide area monitoring system.

I. INTRODUCTION

Power system security assessment (PSSA) is a vital requirement for the secure operation of power grids. Security is a system attribute that is measured with respect to contingencies. PSSA can be dealt with two different behaviors of a power system, namely static and dynamic. Static security concerns the violation of operating variables at the steady-state post-contingency condition, while dynamic security concerns the system's stability during the transient period following a contingency. By PSSA, one measures the system's ability to withstand contingencies and take remedial action for security improvement [1], [2]. In this respect, defining a proper security index plays an important role. Power systems' sheer size and complexity make PSSA an exceptionally computationally demanding task. Furthermore, to preserve the steadily efficient operation of the power system, its operation must always be kept optimal with a fast and accurate system security system. Due to the inevitable rapid employment of renewable power systems that change the characteristics of the electricity network, an extreme level of complexity with more complex data is imposed on the power system stability. Renewable energy resources present challenges for power system security assessment due to uncertainties in generation and load, limitations of traditional model-based methods, massive data handling requirements, and the need to consider system resilience. The integration of full converter-based renewable energy sources can have an impact on various measures of system dynamics, such as the rate of change of frequency (ROCOF) and frequency nadir, etc. After a disturbance, the dynamic behavior of a power system dominated by conventional synchronous generators differs greatly from that of a system dominated by inverters, and this difference depends on factors such as the level of penetration, the type of disturbance, and the type of RES, etc. Accurate forecasting of renewable generation and load is crucial but remains challenging. Advanced data-driven techniques, such as machine learning, can help address these challenges and improve PSSA [3], [4], [5], [6], [7].

PSSA can be carried out in two different environments, namely off-line and on-line. Off-line mode of PSSA refers to the process of evaluating the security status of power systems in a planning environment. In this mode, the steady-state and dynamic performance of near-term predicted scenarios are analyzed to evaluate the current and/or near future security status of power systems. Load flow simulations are utilized to assess several potential contingencies, including outages of transmission lines, transformers, or generators with different loads and power generation scenarios [8]. The outcomes derived from off-line mode are utilized to inform decisions regarding long-term and operational planning. Off-line mode is useful for identifying potential security issues and developing strategies to mitigate them before they occur. It is an important tool for power system planners and operators to ensure the reliability and security of power systems [1]. However, it does not provide real-time information on the power system's behavior, and therefore may not be suitable for detecting and responding to sudden changes or disturbances in the system. On-line PSSA plays a vital role in secure operation of power systems that need on-line data and can be performed by either model-based approaches or measurement-based approaches [9]. In the model-based approaches, which mainly rely on simulation studies using system models, establishing an accurate model for all system components and providing proper parameters for models, are the most challenging tasks which can affect the accuracy and applicability of these approaches. As the main core of these approaches, simulation studies are generally time-consuming, making them less suitable for on-line assessment. Simulation time is always regarded as an essential bottleneck in on-line security assessment [10]. On the other hand, the measurement-based approaches that mainly rely on the on-line measured data without any need for simulation study and system models face the challenge of providing and processing a massive amount of data. In the measurement-based approaches, the measured data should be processed in such a way that security indices can be evaluated with acceptable accuracy. The main advantages of the measurement-based approaches with respect to model-based approaches can be summarized as follows.

- No need to model system components
- No need for parameter data for the model of components
- No need for simulation studies to evaluate system security indices

It is worth noting that the effect of all characteristics such as linear, nonlinear, continuous, discreet and limitation function of system components are naturally reflected in the actual behavior and operating variables of power systems. Therefore, measured data of operating variables include all these characteristics and can be a complete and realistic representative of system attributes like security.

However, due to a considerable amount of data continuously generated in time domain behavior of the power system for operating variables, the measurement-based approaches should be able to handle and overcome the following challenging issues [8], [11].

- Measuring and gathering synchronized online data of operating variables from all over the power network

through wide area monitoring system (WAMS). Without synchronized measured data of the whole network, it is challenging to capture different snapshots of the system behavior, especially during dynamic periods.

- Extracting the most relevant data with respect to each security attribute of the power system as dominant features. Power system security can be analyzed from different aspects with different attributes. However, with respect to each attribute, all operating variables are not involved and contributing. Regarding this fact, to make the estimating process more efficient and faster, it is necessary to eliminate the irrelevant and redundant data and extract the dominant feature with high functionality with the specified attribute.
- Defining security indices that can clearly represent the security status of the power system. In order to assess system security in terms of operating data, it is important to define security indicators that can evaluate the security situation of the power network. To achieve this aim, different indices have been proposed so far.
- Preprocessing the online operational data to assess the security status of the power network. The measured operating variables are the only source available for security evaluation in the measurement-based approaches. The accuracy of the estimation strongly depends on the accuracy of the data [12]. For this purpose, identifying and correcting missed data and erroneous data is vital.
- Developing an estimating tool for establishing a functionality between operating data and security indices. In the non-model-based approaches, to evaluate security indices by the measured operating data, it is required to establish a functionality between each security index and its associated dominant features. For this purpose, different approaches are proposed by using different techniques such as regression, artificial intelligence (AI), and classification.

Considering the foregoing investigations, the traditional security assessment approaches have evidently failed to provide an effective and timely PSSA performance, making it vital to carry out a fast and accurate real-time PSSA. On the other hand, data-driven-based PSSA approaches have been found to be effective and reliable tools, demonstrating promising performance in recent years. An overview of machine learning techniques for analyzing the stability and security of power systems was presented in [13] and [14]. The authors investigated the limitations of the employed classifier design, dataset, and test systems. However, they have only considered the dynamic PSSA, and no investigation has been carried out on the static PSSA. In another work [15], the authors investigated the definitions and dimensions of PSSA. However, they have investigated the systems' security as per the economy, availability, reliability, and sustainability dimensions, and not the assessment methods. Authors in [2] explored the traditional and soft computing-based approaches for PSSA and enhancement. A review of available machine learning technologies for fault and load forecasting in power systems was presented in [16]. According to the authors, a critical challenge in the power systems' fault forecasting is the lack of fault data to train due to the rare fault scenario. However, early detection of a fault or disturbance can produce acceptable results using machine learning technologies. The critical deficiency of [2] and [16] is that the authors have only mentioned the literature that lacks the comparison of the mentioned approaches. Authors in [8] reviewed the application of numerical and machine learning-based approaches for static PSSA. They considered the static security status classification, such as classifiers' types, the static security index, and feature selection and extraction methods. However, despite the great review of static PSSA, the work lacks a comprehensive comparison of the advantages and disadvantages of the reviewed literature. In addition, only the static PSSA is considered, and the dynamic PSSA is not investigated. In this paper, to provide a wide view about the above-mentioned issues related to measurement-based security assessment, all machine learning techniques and approaches concerning this area (as illustrated in Fig. 1) have been comprehensively reviewed.

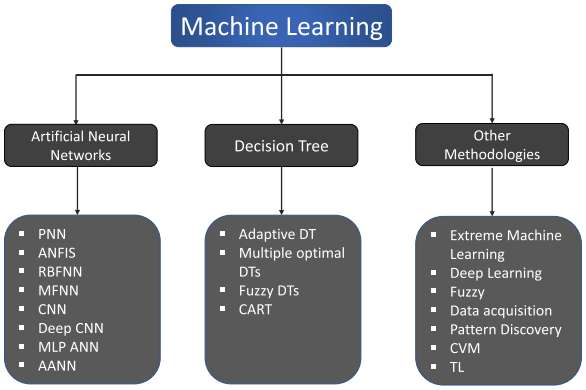


FIGURE 1. Machine learning-based approaches studied for PSSA.

The rest of the paper is organized as follows. Section II is devoted to investigating the PSSA, while the rest of the paper presents a survey of research studies on data-driven PSSA approaches such as artificial neural networks (Section III), support vector machines (Section IV), decision tree (Section V), extreme machine learning, deep learning, fuzzy systems, data acquisition, pattern discovery, and transfer learning (Section VI). Finally, Section VII concludes the paper.

II. SECURITY ASSESSMENT

The process of PSSA involves identifying emergency situations where the power system exceeds its limits during normal (pre-contingency) or potential (post-contingency) operations, as outlined in [17]. PSSA comprises of three primary tasks: security monitoring, contingency analysis, and security control. The security monitoring system provides operational engineers with information about the system's operating condition. The contingency analysis includes contingency

screening and ranking based on the severity obtained from network variables that performs a critical function in the PSSA. Security control aims to reduce the risk of system malfunctioning by selecting appropriate control actions. Stemming from deregulation, modern utilities operate their systems in more stressful operating conditions close to their security limit than they had previously [18]. Accordingly, any disturbance could undermine the systems' security and lead to their collapse under such fragile conditions.

Security analysis can be generally categorized as static security assessment (SSA) and dynamic security assessment (DSA). The first method investigates instances where system limits are exceeded after power outages, but it assumes that the power system returns to a stable state after these outages have occurred, while the latter evaluates the system's performance as it progresses after a disturbance [19]. Further classifications of DSA include pre-fault and post-fault assessments. Pre-fault security assessment utilizes current steady-state variables such as bus voltages, line flow, load, and generation to assess the system's security status before an anticipated disturbance occurs. On the contrary, the post-fault assessment includes characteristics such as voltage trajectory, rotor angle/speed, and a vast area to assess the security status after a fault has occurred. Transient stability analysis (TSA), on the other hand, is a necessity for securing and maintaining the power system's operation, which bolds the criticality of accurate and robust TSA in DSA [20]. The DSA approach aims to deliver the energy management system operators a tool for TSA to be used online, during the normal cycle of real-time operation, and offline for study and research. DSA research falls into three areas: simulation (numerical integration method, direct or Lyapunov methods, and probabilistic), heuristic (expert systems), and database or pattern matching approaches [21]. The ability of a power system to reach a new steady-state operating point without violating the system's operating constraints is called static security [22]. In this context, an operating system's ''static security'' is defined as the bus voltage magnitudes and generated power of generator buses being within their limits, without a line overload [23]. In the SSA technique, the severity of a post contingency scenario is investigated, including the execution of various load flow methods for the base case and the N-1 line outage scenarios. However, they impose time-consuming complexities on the system, and the system operating conditions change over time, making them infeasible for online implementation [24].

Traditional security assessment methods rely on running continuous flow and transient stability simulations, which may not provide the necessary security assessment. For instance, the direct methods using transient energy functions (TEFs) substitute the numerical integrations by stability criteria. Also, probabilistic methods calculate the probability distributions of system stability, which can be computationally intensive, so they are only applicable to power systems planning [25]. On the other hand, modern power systems have grown increasingly complex, making it difficult to assess their online security using traditional methods. As a result, full simulation methods often take too long for online analysis of large power systems with many contingencies to evaluate, even with multiple CPUs [26]. Therefore, there is an emerging demand to develop fast online efficient security assessment approaches capable of monitoring the systems' security under variable conditions to reduce the vulnerability of the systems against various contingencies and ensure safe power system operation.

Due to some remarkable characteristics such as learning and predicting capabilities as well as fast and accurate relationship mapping performance between the power system operating parameters (input) and the corresponding security condition (output), intelligent data-driven approaches can be counted as viable solutions with respect to the traditional approaches. Furthermore, these techniques (such as neural networks, decision trees (DTs), and reinforcement learning-based approaches) are highly effective at identifying important system characteristics that were previously unknown, providing a significant level of insight and discovery [27].

In a data-driven power system security assessment, the machine learning model needs to be trained on a diverse set of data to perform well under various operating conditions. Generating and collecting such data can be a challenge due to the following reasons:

- Diversity of data sources: Power system data can come from various sources, such as generation units, transmission lines, distribution networks, and end-user consumption patterns. Collecting and integrating data from these various sources can be a complex task [28].
- Data quality and consistency: Data collected from different sources may have varying levels of quality, accuracy, and consistency. Ensuring that the data used for training the machine learning model is of high quality and consistent is crucial for the model's performance. Due to security concerns, overcrowding, breaches, and other issues, real power system data may be limited or unavailable for researchers. As a result, they frequently use open source data and simulated data sets in their power system research. Unfortunately, the differences between the available data and the actual power system data can result in inconsistencies in classifications and forecasts [29].
- Temporal and local variability: Power system data can exhibit significant temporal and local variations due to factors such as weather conditions, equipment failures, and changes in consumption patterns. Generating data that captures these variations is essential for training a robust machine learning model [30].
- Data labeling and ground truth: In a supervised learning approach, the training data needs to be labeled with the correct outcomes (e.g., secure or insecure power system states). Obtaining accurate ground truth labels for the data can be time-consuming and labor-intensive [31].

Moreover, there are several database generation methods for training machine learning models in data-driven power

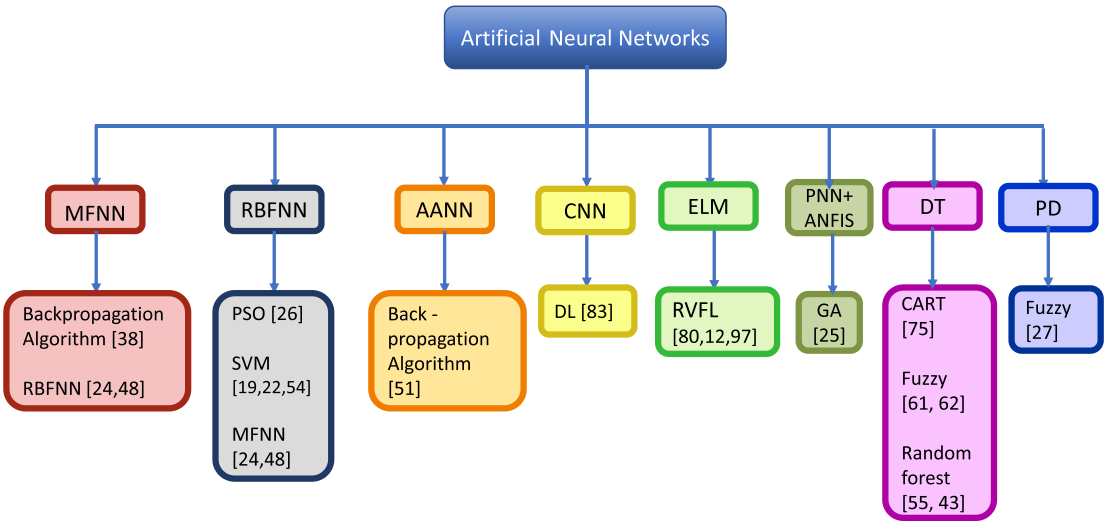


FIGURE 2. Artificial neural network-based approaches studied for PSSA.

system security assessment. These methods aim to provide a diverse and representative dataset for the model to learn from. Here are some methods for generating a database:

- Historical data collection: historical data refers to the operating records of power systems that have been collected over time. These records contain information about actual events that have occurred in practical power systems, such as transient events or disturbances. By analyzing this historical data, we can gain insights into the behavior of power systems and use it to improve dynamic stability assessment [30], [32].
- Importance sampling: Importance sampling is a technique that approximates the maximum likelihood solution for ML-based DSA, reduces the variance in estimated statistics, and avoids the problem of multi-dimensional searching by sampling from a distribution that is more similar to the target distribution. It generates an efficient training database for security assessment by intensively sampling conditions near a security boundary, thereby minimizing computational costs [33], [34].
- Random sampling: The Monte Carlo simulation is a popular technique can be used to generate various random scenarios based on predefined probability distributions for various parameters, such as load levels and generation patterns. Synthetic data can be generated by simulating power system operation under different conditions using power system simulation software. This data can be used to augment the historical data and provide a more diverse dataset for training machine learning models. This method helps to capture the uncertainty in power system operation and ensures a diverse set of data points for model training. By analyzing the statistical properties of the generated samples, machine learning models can be trained to make accurate predictions of system behavior under different operating conditions [34], [35], [36].

By using a combination of these database generation methods, it is possible to create a diverse and representative dataset for training machine learning models in data-driven power system security assessment [37].

III. ARTIFICIAL NEURAL NETWORKS

With the high computation speed and generalization capability of artificial neural networks (ANNs), they have been used in various power system problems, where the conventional approaches fail to achieve the desired accuracy and efficiency. ANNs use an iterative mathematical algorithm to identify intricate connections between an initial state and a final state [21]. Accordingly, with the quick and accurate system security prediction performance, they have found feasible solutions for modern power systems' security monitoring [38]. Figure 2 illustrates a combination of various ANN-based approaches being used individually or collectively in the literature.

A. DYNAMIC

Authors in [39] investigated the ANNs application through power system DSA, considering the system vulnerability as a framework. The authors used the technique for fast pattern recognition and system dynamic security status classification. As reported, the developed scheme demonstrated desirable performance in seven operating conditions along with nine fault locations in an IEEE 50-generator test system. In another study [40], the authors performed the power system security assessment utilizing an augmentation of feature selection techniques and Fisher's linear discriminant as a means for selecting neural network training features. Comparative investigations were provided, and the proposed approach's performance was validated on the IEEE 50-generator transient stability test system, and its superior performance security assessment performance was demonstrated. Authors in [41] proposed a time-frequency-based strategy for rapid

stability assessment and single/multiple contingency severity ranking in power systems. In this context, some strategic monitoring buses were selected, and fuzzy logic and NNs were utilized to determine the initial decisions to improve the assessment reliability and security. In addition, During detailed time-domain simulations, phasor measurement units (PMUs) were installed to record accurate voltage magnitudes and angles. Performance validations on the 67-bus fictitious system and 783-bus system were carried out, where as reported, The proposed strategy showcased superior results with a total of 1027 contingencies derived from two distinct test systems.

An adaptive artificial neural network-based approach was proposed in [21] to predict the generator rotor angle and enhance the power system stability. The approach was augmented with feature selection and data extraction methods to maximize the models ability to generalize and reducing its number of inputs. Although the developed method was reported to decrease the time necessary for DSA, some major limitations still stand with the investigated study, such as no generators were installed into the system to enhance the power system security, and the newly installed generators and shunt capacitors were not monitored. In this context, authors in [42] took advantage of a support vector machine (SVM) classifier and proposed a rotor angle stability prediction paradigm to take the similarity values calculated at the different generator buses as inputs. According to the authors, the developed method was able to predict the transient stability status with a high level of accuracy. Later, A neural network robustness, scalability, and accuracy assessment in power systems was investigated in [43]. In order to verify the cost-effectiveness of the developed paradigms, some verification problems were formulated as mixed-integer linear programs, where the developed methods were used to treat both N-1 security and small-signal stability in the IEEE 9-bus, 14-bus, and 162-bus systems. Comparative investigations in terms of accuracy and rapidity have been carried out with the conventional ANN approach, and the developed method's superior performance was demonstrated.

Authors in [44] presented a hybrid network reduction based on ANN and Ward equivalent approach for online voltage security assessment. As reported, due to the good adaption of the equivalent parameters according to the line status in the buffer zone, the new equivalents scheme demonstrated a desirable response of the external system to the contingencies of the internal system. Later, a dynamic security assessment and generation rescheduling method was proposed in [25] for the preventive control of large power systems against transient instabilities. The authors employed probabilistic neural networks (PNNs) to calculate the security regions. At the same time, an adaptive neuro-fuzzy inference system (ANFIS) -based genetic algorithm (GA) was implemented to reschedule the security-constrained generation. According to the authors, the developed methodology demonstrated a preferable execution speed and accuracy through classifying the system's security. However, despite the satisfactory overall classification performance, missed alarms can lead to undesirable security problems during the assessment and the rescheduling processes. An automatic learning framework for the dynamic security control of power systems was investigated in [26]. The authors utilized a radial basis function neural network (RBFNN) to simultaneously evaluate the power system's dynamic security status and predict the effects of corrective control actions during disturbances. In addition, feature reduction techniques were employed to deal with the large database dimensionality problem. As the authors reported, the developed paradigm was able to effectively choose from all pre-disturbance steady-state variables, resulting in less unnecessary load shedding and more precise identification of vulnerable states. This method proved to be more efficient and outperformed previous techniques [45], [46] methods. Accordingly, the developed method could be used for all instability phenomena, such as voltage, frequency, and rotor angle instabilities.

B. STATIC

Authors in [47] proposed an ANN-aided security assessment approach using a Kohonen self-organizing feature map for a model six-bus power system. Later in [24], the authors employed the multi-layer feed-forward neural network (MFNN) and RBFNN for the online static security assessment of power systems. They used the Newton-Raphson load flow analysis to predict the active power and voltage performance indexes for variable loading conditions under line outage contingencies. The developed approaches' performance was testified using the standard IEEE 30-bus test system. Accordingly, accurate and robust severity prediction and contingencies' ranking performances were reported for unseen network conditions. Authors in [48] developed an online power system static security assessment approach using multi-layer feed-forward ANN and RBFNN networks. The loading conditions and the probable contingencies were considered as inputs to the ANNs. To evaluate the security of the system, the ANNs observed the credible contingencies and prioritized them based on their level of severity. This prioritization was determined by the composite security index, taking into account line flow and bus voltage limit violations. As the comparative studies with conventional methods reported, the developed approach demonstrated faster and more accurate assessments of the system's security against outages.

In order to perform a fast static security assessment, a data mining-based deep convolutional neural network (deep CNN) was developed for static system security assessment with N-1 contingency [49]. In contrast to alternative data-driven methods [50] utilize system state variables to determine the security status of the system, the presented approach depended on the system's topology and bus power injection, which considerably reduced the computational effort. In another study [51], the authors developed an enhanced adaptive ANN approach for security enhancement of Malaysian power grids considering generation dispatch

and load shedding. The developed strategy took advantage of automatic data generation systems and feature selection and data extraction methods to produce AANN inputs. Moreover, varying base load conditions and generation aspects were considered to estimate the remedial control action, where the retraining for new loading scenarios was avoided during the contingencies' severity ranking procedure. An adaptive ANN-based reliable method for power system steady-state security enhancement was proposed in [52]. The presented work alleviated the bus voltage violation and delivered an automatic data knowledge generation method for the adaptive ANN. Comparative performance validations in 9-bus and 39-bus test systems were provided. As reported, the developed method successfully outperformed the conventional methods in mitigating an insecure situation resulting from credible contingency and providing immediately required amounts of generation re-dispatch and load shedding in megawatts.

Table 1 summarizes the security and model types, investigated methods, advantages, and disadvantages of the above-discussed ANN-based PSSA methodologies.

IV. SUPPORT VECTOR MACHINE

Stemming from the statistical learning theory, the SVM constructs a framework capable of employing linear function assumption in a high-dimensional characteristic space [53]. SVM benefits from the structural risk minimization principle leading to less training samples requirement, and has been known as an efficient tool for dynamic and static power system security assessment [19], [22], [53].

A. DYNAMIC

An ensembled SVM-based online security assessment paradigm was proposed in [19]. The developed method incorporated online measurement data obtained from PMUs with multiple linear SVM learners with low computational complexities. A boosting approach was also used to compensate for the inevitable classification errors of linear SVMs. Numerical performance validations were conducted, and as reported, the developed paradigm delivered high and accurate security assessment efficiency. Authors in [53] mapped the online power system transient stability assessment problem as a two-class classification problem. They developed a data mining algorithm, the core vector machine (CVM), to deal with the PMU-based measurements data. The training procedure was carried out in offline mode, and once the CVM was well-trained, the online PMU data was implemented to perform the stability assessment. As the authors reported, the developed CVM successfully outperformed conventional SVM approaches with higher precision and computational burden.

B. STATIC

A SVM-based binary classification scheme was proposed in [54] for static and transient security assessment of IEEE 57-bus and 118-bus power systems. As reported, the developed method considered single line outages as contingencies and outperformed the conventional least square classification method in terms of security evaluation. Later in [22], an online static and transient security assessment approach was proposed using a multiclass SVM classifier. The authors used the sequential forward selection method for the feature selection process. They classified the security status of any given operating condition into four secure, critically secure, insecure, and highly insecure modes. As the comparative simulation results with least-squares, probabilistic neural network, extreme learning machine, and extreme SVM classifiers reported, the proposed scheme demonstrated superior online static and transient security validation with low computational time performance, making it suitable for online static and transient security validation and computational time for practical implementation.

Table 2 summarizes the security and model types, investigated methods, advantages, and disadvantages of the above-discussed SVM-based PSSA methodologies.

V. DECISION TREE

The decision tree is a well-established data mining and classification approach being used for various high-dimension and big data problems. DTs benefit from a unique feature that utilizes the thresholds of attributes (linear classifiers) to predict the considered objective. Hence, many researchers have utilized DTs for both online and offline power systems security assessment problems [55], [56], [57], [58].

A. DYNAMIC

A scheme was suggested to assess voltage security in real-time, with the aim of identifying security issues that may arise after a contingency event, including voltage magnitude violations and voltage and transient stability [56]. Later in [59], a similar approach was developed to deal with the same problem. However, the authors implemented an augmentation of synchronized phasor measurements and periodically updated DTs. The DTs were trained offline hourly, considering the voltage security analysis conducted during the past representative and 24-h ahead operating conditions forecasts. Accordingly, to assess security, the offline thresholds determined by the DTs were compared to the online-obtained synchronized critical attributes PMUs. Performance validations were carried out on the American Electric Power (AEP) system, and as reported, the developed strategy demonstrated suitable voltage security assessment performance. An online PMU and DT -based dynamic security assessment approach for large-scale interconnected power systems was proposed in [60]. Online security assessment and preventive control guidelines supplemented by real-time PMU data were created by authors via the utilization of DTs. Since the security predictions based not the terminal nodes lack validity if any unpredictable system conditions occur, they used a classification method considering each whole path of a DT instead of classification results at terminal nodes to enhance its performance and

TABLE 1. Summary of ANN approaches for PSSA.

Ref.	Security type	Model type	Method	Advantages	Disadvantages
[44]	Dynamic	Model-based	MLP ANN	Robustness against input and system disturbance, Online identification of external system	Requires large training sets for a reliable assessment, MLP parameters design problem
[25]	Dynamic	Model-based	GA-based Probabilistic NN	No requirement for large training sets, Low computational complexity	Relatively slow due to the optimization process
[21]	Dynamic	Model-based	Adaptive ANN	Fast security assessment, Applicable even when the system configuration is changed	Only the changes in the transmission lines and load demand are considered, It is assumed that no generators are installed into the system
[26]	Dynamic	Model-based	PSO-based RBFNN	Applicable during voltage, frequency, and rotor angle instability, Giving a measure of reliability of the DSA, High speed performance	High computational complexity, Better optimization algorithms can overtake PSO with better performance, Requires large training sets for a reliable assessment
[24]	Static	Model-based	Multi-layer feed forward NN and RBFNN	Fast, accurate, and robust security evaluation performance for unseen network conditions, Low computational effort	High reliability on the NN design and parameters, Exhaustive training process
[47]	Static	Model-based	Self-organizing ANN	–	Requires large training sets for a reliable assessment
[39]	Dynamic	Model-based	ANN	Ability to provide the severity indices accurately	High reliability on the NN design and parameters, High computational time
[49]	Static	Model-based	Deep convolutional NN	No requirement for system state variables, Low computational complexity	–
[51]	Static	Model-based	Adaptive NN	Reduction in the count of inputs/outputs is achieved through power system network clustering, Low computational complexity, Varying base load conditions considered	Exhaustive training process for large-scale power system
[48]	Static	Online	Multi-layer feed-forward ANN, RBFNN	Low computational effort in online security assessment	Not all possible contingencies are considered, and only the first ones of the ranking
[40]	Dynamic	Model-based	ANN	Good performance under conditions of unforeseen changes in system topology	The method requires an optimal number of pre-defined features to search for, which is a difficult task
[52]	Static	Model-based	Adaptive ANN	Fast and accurate estimation of generation re-dispatch and load shedding values, Good performance on large-scale power systems	–
[38]	Static	Model-based	Multilayer feed-forward NN with backpropagation algorithm	Less error and required time compared to Newton-Raphson algorithm	Inferior performance compared to Newton-Raphson algorithm, Exhaustive training process

TABLE 2. Summary of SVM approaches for PSSA.

Ref.	Security type	Model type	Method	Advantages	Disadvantages
[19]	Dynamic	Online	Ensemble of multiple linear SVMs and AdaBoost algorithm	Simplicity of implementation, Fast computation, Overcomes the classification errors of individual linear SVM	High sensitivity to the SVM tuning parameters
[22]	Dynamic & Static	Model-based	Multiclass SVM, Sequential forward selection (SFS) as feature selection, RBF as the kernel mapping function, SVM parameter selection by differential evolution (DE) algorithm	Good preventive control performance, Highly accurate classification, Low computational time	High sensitivity on proper selection of the input feature set
[54]	Dynamic & Static	Model-based	RBF kernel function in the SVM model, SVM based Pattern Recognition approach, SFS as feature selection	Highly accurate classification	Its efficacy is limited to classes that can be separated linearly
[53]	Dynamic	Online	CVM	Higher precision and lower computational complexity as compared to SVM	–
[20]	Dynamic	Online	Multi-layer SVM ensemble and stacked denoising auto encoder (SDAE), deep learning (DL) for feature extraction based on SDAE	Higher accuracy compared to SVM due to converting the weak learners to strong learners using voting technique	–

ensure more reliability. Authors in [61] and [62] proposed fuzzy DT-based power system security assessment schemes capable of dealing with uncertainties and large-scale problems. The developed methods combined the advantages of conventional DTs with NNs [61] and PMUs [62] and avoided their disadvantages. Consequently, desirable compromises between interpretability and accuracy were achieved.

Another work [57] investigated a PMU-based power system transient stability and voltage stability approach. The authors used DTs to identify the critical attributes to be measured by PMUs, and as a result, characterized important phenomena associated with system dynamic performance. According to the authors, the proposed scheme could deliver more reliable security predictions based on all nodes of the related paths of the DTs. Aiming at mitigating the impact of missing PMU data, an ensemble DT-based data mining scheme for online DSA was developed in [58]. The authors used a random subspace method to exploit the locational information of attributes and the availability of PMU measurements; and trained multiple small DTs. A boosting algorithm was utilized to quantify the voting weights of viable small DTs, and utilized the re-check results to re-weight the DTs in the ensemble. According to the authors, the developed approach achieved superior performance than conventional DT-based techniques. In another study [63], a PMU-based voltage security assessment paradigm was proposed to maintain the steady voltage magnitudes at all buses in the power system subjected to disturbances. They took advantage of an adaptive ensemble Hoeffding tree-based learning [64] to guarantee the robustness of the proposed technique. According to the authors, the developed method could effectively reduce the computation burden and deliver lower misclassification errors than the traditional DT method.

Authors in [45], [65], and [66] proposed a DT-based DSA with corrective control performance. Security regions and

system status were determined through the DTs implementation. Accordingly, the scheme could provide guidelines to take the necessary preventive or corrective control to address transient instabilities. Later in [67], a DT-based approach for preventive control and online power system DSA was developed. The authors trained two contingency-oriented DTs for power systems with high penetration of wind generation and other distributed generations (DGs), where a DT was employed to identify potential security issues during DSA, and the other one provided the operators with online decision support on preventive control. In order to simultaneously ensure the maximum database information and minimize the computing requirements, an efficient DT-based sampling strategy was proposed in [68]. As the author reported, the comparative studies demonstrated an extensively improved classification performance of the developed approach than that of conventional sampling methods, leading to more accurate power system security assessments. Later, authors in [69] proposed two optimization-based DT approaches to improve the interpretability of the DT-based dynamic security rules. According to the comparative investigations, the proposed approaches demonstrated superior predictive performances and interpretability of the security rules with less required training data. This characteristic leads to a reduced offline computational burden of dynamic security assessment platforms. Authors in [70] proposed a contingency-based DT approach to analyze the impact of wind energy and cross-border power exchange on the dynamic security of present and future Danish power systems. The security assessments were carried out offline for many possible operating conditions, and the database was made using the critical contingencies. The built-up database was then used for security prediction of present and future power systems.

A DT-based online voltage security assessment scheme focused on voltage collapse problems caused by severe disturbances was proposed in [71]. The authors simulated an N-1 contingency case for each considered operating scenario, and real-time measurements were carried out periodically to update the system information. As reported, using the developed scheme, the power system states were efficaciously ranked with respect to their potential for causing voltage instability. Authors in [65] combined wide-area measurements and DT algorithms to develop an online voltage security assessment strategy. Despite the developed paradigm's acceptable accuracy on the reduced database, it could not deliver the desired accuracy when dealing with the original database. Hence, the authors employed an adaptive boosting method to combine individual DTs and achieve an accurate prediction. As reported, the developed model demonstrated a preferred performance in the presence of uncertainty in the load and generation variation scenarios.

B. STATIC

Aiming at achieving a more precise power system security assessment for multiple contingencies, authors in [72] developed a multiway DT-based approach with reduced decision nodes. Compared to conventional DT methods, the proposed scheme is less sensitive to variations, and the computational burden is reduced due to fewer decision nodes. However, more detailed comparative investigations are needed to be carried out to validate its practical viability. Data-mining-based robust online DSA schemes were proposed in [73] and [74] by considering the operating condition variations and topology changes of power grids. The developed schemes used raw measurements reported by PMUs, where classical DT [74] and adaptive ensemble DT [73] learning strategies were utilized to assess the security of practical power systems. As reported, improved performance in terms of accuracy and cost-effectiveness was achieved compared to conventional methods.

Table 3 summarizes the security and model types, investigated methods, advantages, and disadvantages of the above-discussed DT-based PSSA methodologies.

VI. OTHER METHODOLOGIES

A. EXTREME MACHINE LEARNING

The conventional learning methods are based on a single learning model, which has resulted in high computational time and low accuracy when dealing with big data analysis. Extreme machine learning (EML) approaches learn without any time-consuming adjustment of network parameters have enhanced the conventional methods' accuracy with much less computation memory [78]. These features have made EML approaches efficacious tools for online security assessment of large power systems. According to the literature, it is noteworthy that EML approaches are only used for DSA, and no studies have been found on SSA.

A real-time ELM-based DSA approach was proposed in [78]. To validate the effectiveness of the developed approach, it was conducted on an IEEE 50-machine system and a dynamic equivalent system of a real-world large power grid. Taking advantage of the developed approach, fast estimation performance was reported with 100% classification accuracy and a reliable pre-fault DSA mechanism. Authors in [79] developed an online data-driven DSA paradigm to accommodate rapid and volatile wind power variations considering foreseeable disturbances. Practical investigations were conducted, where the developed DSA scheme delivered high DSA efficiency and accuracy. Later in [80], a multiple randomized learning-based ensemble model was proposed to deal with online DSA. To achieve faster learning capability and more reliable machine learning outcomes, the authors combined extreme learning machine and random vector functional link networks (RVFLNs) for the problem at hand. Another study [12] investigated a PMU-based pre-fault DSA with incomplete data measurements using a generative adversarial network. Despite the conventional methods that depend on PMU observability for the missing data, the authors in [12] utilized the generative adversarial network to address the incomplete data. According to the provided investigations, the method demonstrated high DSA accuracy

TABLE 3. Summary of DT approaches for PSSA.

Ref.	Security type	Model type	Method	Advantages	Disadvantages
[63]	Dynamic	Online	Adaptive DT	For updating, this approach only requires the most recent data updates and basic statistical analysis instead of the entire dataset, Low computational complexity, Low misclassification error	Only one contingency considered
[59]	Dynamic	Online	Multiple optimal DTs	Good security assessment performance	Increased computational complexity and time
[71]	Dynamic	Online	Random forest-based DTs	Good security assessment performance	Only one contingency considered
[67]	Dynamic	Online	Contingency-oriented DTs	Fast online situational awareness	High dependance of the method's accuracy and reliability on the learning data set
[75]	Dynamic	Online	Classification and regression trees (CART), ANN	Good security assessment performance, Low computational complexity	–
[57]	Dynamic	Online	CART	Provides reliable assessment performance against perturbations of operating conditions	–
[61]	Dynamic	Online	Fuzzy DTs, MLP ANN	Provides more refined and accurate information about system security	–
[56]	Static	Online	CART	Good security assessment performance	Not realistic load model used
[72]	Static	Online	Multiway DT, Stratified random sampling	Provides reliable accurate assessment performance	Slightly higher computational complexity compared to that of DT
[76]	Dynamic	Online	Integration of DT and case-based reasoning	Fast security assessment performance, Low computational complexity	Considers a single machine connected to an infinite bus
[62]	Dynamic	Online	Fuzzy-based DT	More flexibility in the tuning of decision boundaries compared to that of DT , Good stability assessment performance	–
[73]	Dynamic	Online	Adaptive DT	Highly accurate security assessment performance	Increased computational complexity, Time consuming
[55]	Dynamic	Model-based	Bagging (random forest) and AdaBoost methods	Improved accuracy compared to that of DT	Slightly increased computational complexity
[77]	Dynamic	Model-based	Multiple DTs, XGBoost -based TSA	Provides fast and reliable assessment performance	Only one contingency considered

with a much less computation complexity under any PMU missing conditions.

B. DEEP LEARNING

As one of the most recent and powerful learning techniques, deep learning approaches have successfully merged into research and industry fields, overcoming other machine learning approaches [81], [82]. Deep learning approaches can automatically extract effective features for different tasks and have demonstrated remarkable performance when dealing with large amounts of data. Accordingly, these approaches have been found effective solutions for data-driven security assessment of large power systems [12], [20], [83], [84].

A deep learning-based feature extraction framework with enhanced training performance was proposed in [82] to assess power systems' security. The training procedure was improved utilizing an R-vine copula-based sampling strategy, while deep autoencoders were employed to reduce the high-dimensional input space of security assessment. According to the provided performance validations, the developed strategy demonstrated a suitable security assessment performance. In another study [83], using convolutional neural networks and deep learning, a power system security assessment paradigm was developed to assess N-1 security and small-signal stability on the NESTA 162-bus system. As reported, owing to representing the power system snapshots as images, the convolutional neural networks could easily process the data, resulting in a much faster and more accurate security assessment than the standard small-signal stability assessment method. A PMU-based pre-fault dynamic security assessment approach considering the incomplete data measurements was developed in [12]. The authors employed the deep-learning method generative adversarial network (GAN) [84], [85] to address the missing data, where the Adam algorithm [86] was used to pursue the highest assessment accuracy with desirable efficiency. According to the investigations provided and reported by the authors, the developed approach has been found effective in filling up incomplete PMU data independent of PMU observability and network topologies. Later, authors in [20] presented a dynamic security assessment scheme based on SDAE ensembled with boosting learning approach. They employed the multi-layer SDAE to extract the original input data, along with an SVM classifier to perform classification with data from all hidden layers of SDAE. As reported, the developed scheme improved the security assessment accuracy with reduced computational time.

Table 4 summarizes the security and model types, investigated methods, advantages, and disadvantages of the above-discussed EML-based and DL-based PSSA methodologies.

C. FUZZY SYSTEMS

Due to the desirable prediction and analysis performance of fuzzy inference systems (FISs), they have been widely used in many power system security analysis approaches [27], [87], [88]. In this context, the augmentation capability of fuzzy systems with other classic and advanced power system security assessment approaches has established them as useful and effective data-driven methods over the past decade [27], [89]. According to the literature, it is noteworthy that fuzzy-based approaches are only used for DSA, and no studies have been found on SSA.

Authors in [41] proposed an integration of Fuzzy logic and neural networks to improve power systems' security and reliability assessment. The developed scheme's performance was testified on a 67-bus fictitious system and a 783-bus system in actual use at Hydro-Quebec's operations planning department. Later in another study [62], the same authors

TABLE 4. Summary of ELM and DL approaches for PSSA.

Ref.	Security type	Model type	Method	Advantages	Disadvantages
[80]	Dynamic	Online	ELM, RVFLN	Fast security assessment performance, Low number of parameters to tune, Low computational complexity	A single learning algorithm is used that may not fully map the relationships embedded in the training data
[78]	Dynamic	Model-based	ELM decision making, single-hidden layer feed-forward network (SLFN)	Provides reliable accurate assessment performance, Less data requirement compared to those of other ensemble approaches	–
[12]	Dynamic	Online	ELM and RVFLN, DL, generative adversarial network (GAN)	Fast security assessment performance, Low computational complexity, Low number of parameters to tune	–
[79]	Dynamic	Model-based	ELM	Fast security assessment performance	–
[82]	Dynamic	Model-based	DL-based feature extraction, Regular vine (R-vine) copula-based sampling strategy	Can deal with imbalanced data	High computational time, especially under fault scenarios
[83]	Dynamic	Model-based	Convolutional NN (CNN) and DL, Adam optimizer	Faster stability assessment performance compared to standard small-signal, High accuracy	–

TABLE 5. Summary of Fuzzy, PD, and DA approaches for PSSA.

Ref.	Security type	Model type	Method	Advantages	Disadvantages
[17]	Dynamic	Online	Distributed architecture based on the Web	Fast parallel processing-based security analysis	Requires high-performance computational machines
[9]	Dynamic	Online	Spatial-temporal dynamic visualization based on the PMI and IRF	Good preventive control performance, Fast and efficient security assessment	Raises cybersecurity concerns due to its IoT-based configuration
[62]	Dynamic	Online	Fuzzy-based classifier, DT	High tuning flexibility	Excessive training and tuning burdens
[87]	Dynamic	Online	Fuzzy logic	Low computational complexity	Only considers the deterministic values and does not factor in event probabilities or assess the risk level of the system
[41]	Dynamic	Model-based	Fuzzy logic and NN	Accurate security assessment	High computational time, Highly dependable on the design and parameters
[27]	Dynamic	Model-based	PD-based fuzzy	Good prediction performance	Raises cybersecurity concerns, and prone to communication failure
[89]	Dynamic	Model-based	PD	Good prediction performance	Raises cybersecurity concerns

proposed a rapid power systems' stability assessment scheme using transparent fuzzy rule-based classifiers initialized by large-size accurate decision trees. Phasor measurement units were used to capture real-time wide-area response signals in power system operation. These signals were then analyzed in both the time and frequency domains to extract vital decision features, including the highest spectral density of the angle, frequency, and the dot product of these variables evaluated across the entire power grid. Owing to the fuzzy-rule classifiers, highly efficient fast contingency screening with reduced computation time was reported according to the validations provided on a large database of the Hydro-Quebec grid. Authors in [27] developed an enhanced semi-supervised pattern discovery method augmented with a fuzzy classification scheme for dynamic security assessment of power systems. They used the fuzzy classification scheme to predict the security index of the power system operating point. Comparative performance investigations of the developed method were carried out on the IEEE 50-bus system, where the method outperformed other classification techniques [41], [61]. In addition, taking advantage of the enhanced pattern discovery method, the developed method was reported more efficient in power systems security assessment than [89], with faster assessment speed than [87].

D. DATA ACQUISITION

A web-based distributed architecture for real-time security assessment, data acquisition, and safety check violations of power systems was developed in [17]. The authors analyzed system's security by using a network of remotely controlled units that were placed in the most critical sections of the power grid with a Web-based interface to report the development. However, although the developed paradigm was reported to provide a viable online security analysis solution of electrical networks, more efforts are needed to validate its performance in dealing with variable and very large networks. SCADA measurements play a crucial role in power system monitoring and control. However, they may not be sufficient for a comprehensive power system security assessment due to limited coverage, failure to capture system dynamics in real time, errors, outdated equipment models, attack surface vulnerabilities, have a fixed sampling rate, and lack of forecasting capabilities [2], [90], [91]. To address these limitations, additional data sources such as synchrophasor measurements from Phasor Measurement Units (PMUs) can be used to complement SCADA measurements. PMUs provide high-speed, high-resolution data that can capture transient events and provide a more comprehensive view of the power system. By combining data from multiple sources, power system security assessments can be more accurate and effective in identifying potential vulnerabilities and risks [92]. Authors in [9] proposed an integrated model-free online DSA approach that incorporates feature selection and regression prediction. They employed partial mutual information (PMI) [93] and the Pearson correlation coefficient (PCC) [94] to select critical variables during feature selection, which reduced the dimensionality of the initial database. At the same time, an iterated random forest (IRF) [95] was employed to predict the transient stability margin. The feasibility and performance of the developed method were validated on the IEEE 39-bus and practical

large-scale 1648-bus systems. According to the authors, desirable prediction accuracy with robustness in dealing with missing data and measurement noise was achieved.

E. PATTERN DISCOVERY

Pattern discovery methods are unsupervised learning techniques that can provide visualized explicit assessment solutions for power system operators. These methods can statistically discover multiple hyper-rectangles (patterns) in power system dynamic security databases and consequently can determine the secure/insecure regions of the system [27].

A statistical learning-based technique was developed in [89] for dynamic security assessment and preventive stability control of harmful disturbances in power systems. The authors employed an unsupervised pattern discovery (PD) procedure to extract patterns from a feature space characterized by critical generators. As reported from a practical point of view, owing to the developed unsupervised PD approach, a visualized explicit assessment performance was obtained for power system operators, and the stability assessment was made by a distance-based classification procedure, where the stability control could be realized by driving an operating point from an insecure region to a secure region.

Table 5 summarizes the security and model types, investigated methods, advantages, and disadvantages of the above-discussed fuzzy-based, PD-based, and DA-based PSSA methodologies.

F. TRANSFER LEARNING

In [96], the authors proposed an integrated transfer learning (TL) method for DSA models to address the issues of limited coverage in offline training databases and missing data inputs due to practical issues. The proposed method used adversarial training and feature extractor networks to enhance the extensibility of DSA models, allowing them to cover more unlearned faults with complete or incomplete data. Although the previous works have addressed these issues separately, but the proposed method showed that they can occur simultaneously in practice. The validity of the method was demonstrated through simulation tests on the New England 10-machine 39-bus system using the Monte-Carlo method. The TSA tool was used to carry out a time-domain simulation, which assessed the dynamic security level of each operating point. Authors in [97] developed a data-driven method for dynamic security assessment that can assess multiple faults that were not trained. Based on the transfer learning theory, the method uses Maximum Mean Discrepancy to minimize differences between the distributions of trained and unknown data and combines two randomized learning algorithms, extreme learning machine (ELM) and random vector functional link (RVFL), to improve performance. The proposed method achieved a 97.27% accuracy in fault assessment validation. The method was tested on the New England 10-machine 39-bus system using transient stability criterion to label instances.

VII. CONCLUSION

This paper provided a comprehensive review of the state-of-the-art studies on the data-driven security assessment of power systems. Power systems security evaluation is crucial for security monitoring, contingency analysis, and power system security control. According to the literature, conventional methods have shown deficiencies in terms of resiliency and adaptation to the current and future trends in power systems, which demands the deployment of more reliable power systems security assessment (PSSA) methodologies. In this context, owing to some outstanding characteristics such as fast and accurate learning and predicting capabilities, data-driven approaches have successfully overcome the conventional methods and effectively dealt with the current growth of power networks, large database problems, and the requirement of rapid PSSA, especially in online assessments. This study comprehensively surveyed the application of data-driven approaches such as artificial neural networks, support vector machines, decision tree methods, and various machine learning-based approaches in dynamic and static PSSA.

According to the literature investigations, it was found that AANs can provide online identification of external systems with a high level of robustness against input and system disturbances, delivering a fast and accurate security assessment performance even when the system configuration is changed. However, large training sets are required for a reliable assessment which increases the computational complexity. On the other hand, benefiting from the structural risk minimization principle that leads to fewer training data, SVMs have demonstrated themselves as highly accurate PSSA methods with decreased computational complexity with respect to AANs. However, their main drawback is their high sensitivity to the tuning parameters. As bigger datasets impose more computational complexities, decision tree-based approaches have been found as alternative solutions to deliver reliable and accurate PSSA performance. This stems from their structural concepts that require only the latest updating data and basic statistical analysis instead of the whole data set for updating purposes, which drastically decreases the computational complexity while delivering accurate PSSA. Such data-driven approaches (such as ANNs, DTs, and learning-based approaches) can provide a high degree of discovery, which allows them to uncover salient but previously unknown characteristics of a system. Other useful but less implemented approaches such as ELM, fuzzy, and PD have been found effective to deliver fast and accurate security assessments due to less number of tuning parameters; however, the latter raises cybersecurity concerns, making it not suitable for many PSSA applications. This study contributes to the literature as follows:

- A comprehensive evaluation of the merits and demerits of the literature studies from the data-driven perspective is provided, which can effectively deliver a beneficial insight to researchers concerning the application of data-driven methods for PSSA.

- A complete discussion and evaluation of static and dynamic security assessment from different aspects is provided.
- A wide range of data-driven PSSA approaches is brought under one roof. In addition, a PSSA performance comparison among different artificial intelligent approaches has been carried out.

REFERENCES

[1] E. Abel, G. N. Nyakoe, and C. M. Muriithi, "Techniques of power system static security assessment and improvement: A literature survey," *Heliyon*, vol. 9, no. 3, 2023, Art. no. e14524.

[2] K. Teeparthi and D. M. Vinod Kumar, "Power system security assessment and enhancement: A bibliographical survey," *J. Inst. Eng. India B*, vol. 101, no. 2, pp. 163–176, Apr. 2020.

[3] Z. Yao, Y. Lum, A. Johnston, L. M. Mejia-Mendoza, X. Zhou, Y. Wen, A. Aspuru-Guzik, E. H. Sargent, and Z. W. Seh, "Machine learning for a sustainable energy future," *Nature Rev. Mater.*, vol. 8, no. 3, pp. 202–215, 2023.

[4] P. Sarajcev, "Machine learning in power system dynamic security assessment," *Energies*, vol. 15, no. 11, 2022.

[5] J. Wang, P. Pinson, S. Chatzivasileiadis, M. Panteli, G. Strbac, and V. Terzija, "On machine learning-based techniques for future sustainable and resilient energy systems," *IEEE Trans. Sustain. Energy*, vol. 14, no. 2, pp. 1230–1243, Apr. 2023.

[6] Q. Zhang, X. Li, X. Liu, C. Zhao, R. Shi, Z. Jiao, and J. Liu, "Data-driven risk assessment early-warning model for power system transmission congestions," in *Proc. 12th Int. Conf. Power, Energy Electr. Eng. (CPEEE)*, Feb. 2022, pp. 201–206.

[7] H. Cui, S. Konstantinopoulos, D. Osipov, J. Wang, F. Li, K. L. Tomsovic, and J. H. Chow, "Disturbance propagation in power grids with high converter penetration," *Proc. IEEE*, vol. 111, no. 7, pp. 873–890, Jul. 2023.

[8] M. Gholami, M. J. Sanjari, M. Safari, M. Akbari, and M. R. Kamali, "Static security assessment of power systems: A review," *Int. Trans. Electr. Energy Syst.*, vol. 30, no. 9, 2020, Art. no. e12432.

[9] S. Liu, L. Liu, Y. Fan, L. Zhang, Y. Huang, T. Zhang, J. Cheng, L. Wang, M. Zhang, R. Shi, and D. Mao, "An integrated scheme for online dynamic security assessment based on partial mutual information and iterated random forest," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3606–3619, Jul. 2020.

[10] T. Venkatesh and T. Jain, "Synchronized measurements-based wide-area static security assessment and classification of power systems using case based reasoning classifiers," *Comput. Electr. Eng.*, vol. 68, pp. 513–525, May 2018.

[11] F. Bai, Y. Liu, Y. Liu, K. Sun, N. Bhatt, A. D. Rosso, E. Farantatos, and X. Wang, "Measurement-based correlation approach for power system dynamic response estimation," *IET Generat. Transmiss. Distrib.*, vol. 9, no. 12, pp. 1474–1484, Sep. 2015.

[12] C. Ren and Y. Xu, "A fully data-driven method based on generative adversarial networks for power system dynamic security assessment with missing data," *IEEE Trans. Power Syst.*, vol. 34, no. 6, pp. 5044–5052, Nov. 2019.

[13] Q. Wang, F. Li, Y. Tang, and Y. Xu, "Integrating model-driven and data-driven methods for power system frequency stability assessment and control," *IEEE Trans. Power Syst.*, vol. 34, no. 6, pp. 4557–4568, Nov. 2019.

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

[15] A. Sarhan, V. K. Ramachandaramurthy, T. S. Kiong, and J. Ekanayake, "Definitions and dimensions for electricity security assessment: A review," *Sustain. Energy Technol. Assessments*, vol. 48, Dec. 2021, Art. no. 101626.

[16] Z. Ma, C. Zhang, and C. Qian, "Review of machine learning in power system," in *Proc. IEEE Innov. Smart Grid Technol. Asia (ISGT Asia)*, May 2019, pp. 3401–3406.

[17] M. Di Santo, A. Vaccaro, D. Villacci, and E. Zimeo, "A distributed architecture for online power systems security analysis," *IEEE Trans. Ind. Electron.*, vol. 51, no. 6, pp. 1238–1248, Dec. 2004.

[18] A. Mehrzad, M. Darmiani, Y. Mousavi, M. Shafie-Khah, and M. Aghamohammadi, "An efficient rapid method for generators coherency identification in large power systems," *IEEE Open Access J. Power Energy*, vol. 9, pp. 151–160, 2022.

[19] H. T. Nguyen and L. B. Le, "Online ensemble learning for security assessment in PMU based power system," in *Proc. IEEE Int. Conf. Sustain. Energy Technol. (ICSET)*, Nov. 2016, pp. 384–389.

[20] Rizwan-ul-Hassan, C. Li, and Y. Liu, "Online dynamic security assessment of wind integrated power system using SDAE with SVM ensemble boosting learner," *Int. J. Electr. Power Energy Syst.*, vol. 125, Feb. 2021, Art. no. 106429.

[21] A. N. Al-Masri, M. Z. A. A. Kadir, H. Hizam, and N. Mariun, "A novel implementation for generator rotor angle stability prediction using an adaptive artificial neural network application for dynamic security assessment," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 2516–2525, Aug. 2013.

[22] S. Kalyani and K. S. Swarup, "Classification and assessment of power system security using multiclass SVM," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 41, no. 5, pp. 753–758, Sep. 2011.

[23] L. Wehenkel, "Machine learning approaches to power-system security assessment," *IEEE Expert*, vol. 12, no. 5, pp. 60–72, Sep. 1997.

[24] P. Sekhar and S. Mohanty, "An online power system static security assessment module using multi-layer perceptron and radial basis function network," *Int. J. Electr. Power Energy Syst.*, vol. 76, pp. 165–173, Mar. 2016.

[25] C. F. Kucuktezcan and V. M. I. Genc, "A new dynamic security enhancement method via genetic algorithms integrated with neural network based tools," *Electric Power Syst. Res.*, vol. 83, no. 1, pp. 1–8, Feb. 2012.

[26] E. M. Voumvoulakis and N. D. Hatziargyriou, "A particle swarm optimization method for power system dynamic security control," *IEEE Trans. Power Syst.*, vol. 25, no. 2, pp. 1032–1041, May 2010.

[27] F. Luo, Z. Dong, G. Chen, Y. Xu, K. Meng, Y. Chen, and K. Wong, "Advanced pattern discovery-based fuzzy classification method for power system dynamic security assessment," *IEEE Trans. Ind. Informat.*, vol. 11, no. 2, pp. 416–426, Apr. 2015.

[28] N. V. Tomin, V. G. Kurbatsky, D. N. Sidorov, and A. V. Zhukov, "Machine learning techniques for power system security assessment," *IFAC-PapersOnLine*, vol. 49, no. 27, pp. 445–450, 2016.

[29] A. Sharifzadeh, M. T. Ameli, and S. Azad, "Power system challenges and issues," in *Application of Machine Learning and Deep Learning Methods to Power System Problems*. Springer, 2021, ch. 1, pp. 1–17.

[30] A. Mollaiee, M. T. Ameli, S. Azad, M. Nazari-Heris, and S. Asadi, "Data-driven power system security assessment using high content database during the COVID-19 pandemic," *Int. J. Electr. Energy Syst.*, vol. 150, Aug. 2023, Art. no. 109077.

[31] J. L. Cremer, I. Konstantelos, S. H. Tindemans, and G. Strbac, "Data-driven power system operation: Exploring the balance between cost and risk," *IEEE Trans. Power Syst.*, vol. 34, no. 1, pp. 791–801, Jan. 2019.

[32] L. Zhu and D. J. Hill, "Data/model jointly driven high-quality case generation for power system dynamic stability assessment," *IEEE Trans. Ind. Informat.*, vol. 18, no. 8, pp. 5055–5066, Aug. 2022.

[33] L. Zhu, D. J. Hill, and C. Lu, "Semi-supervised ensemble learning framework for accelerating power system transient stability knowledge base generation," *IEEE Trans. Power Syst.*, vol. 37, no. 3, pp. 2441–2454, May 2022.

[34] K. Hao and Q. Wan, "Importance sampling based direct maximum likelihood position determination of multiple emitters using finite measurements," *Signal Process.*, vol. 186, Sep. 2021, Art. no. 108111.

[35] C. Ren and Y. Xu, "Robustness verification for machine-learning-based power system dynamic security assessment models under adversarial examples," *IEEE Trans. Control Netw. Syst.*, vol. 9, no. 4, pp. 1645–1654, Dec. 2022.

[36] D. Mukherjee, S. Chakraborty, and S. Ghosh, "Power system state forecasting using machine learning techniques," *Electr. Eng.*, vol. 104, no. 1, pp. 283–305, Feb. 2022.

[37] A.-A.-B. Bugaje, J. L. Cremer, and G. Strbac, "Split-based sequential sampling for realtime security assessment," *Int. J. Electr. Power Energy Syst.*, vol. 146, Mar. 2023, Art. no. 108790.

[38] I. S. Saeh and A. Khairuddin, "Static security assessment using artificial neural network," in *Proc. IEEE 2nd Int. Power Energy Conf.*, Dec. 2008, pp. 1172–1178.

[39] Q. Zhou, J. Davidson, and A. A. Fouad, "Application of artificial neural networks in power system security and vulnerability assessment," *IEEE Trans. Power Syst.*, vol. 9, no. 1, pp. 525–532, Feb. 1994.

[40] C. A. Jensen, M. A. El-Sharkawi, and R. J. Marks, "Power system security assessment using neural networks: Feature selection using Fisher discrimination," *IEEE Trans. Power Syst.*, vol. 16, no. 4, pp. 757–763, Nov. 2001.

[41] I. Kamwa, R. Grondin, and L. Loud, "Time-varying contingency screening for dynamic security assessment using intelligent-systems techniques," *IEEE Trans. Power Syst.*, vol. 16, no. 3, pp. 526–536, Aug. 2001.

[42] A. D. Rajapakse, F. Gomez, K. Nanayakkara, P. A. Crossley, and V. V. Terzija, "Rotor angle instability prediction using post-disturbance voltage trajectories," *IEEE Trans. Power Syst.*, vol. 25, no. 2, pp. 947–956, May 2010.

[43] A. Venzke and S. Chatzivasileiadis, "Verification of neural network behaviour: Formal guarantees for power system applications," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 383–397, Jan. 2021.

[44] T. S. Chung and Y. Fu, "A fast voltage security assessment method via extended ward equivalent and neural network approach," *IEEE Power Eng. Rev.*, vol. 19, no. 10, pp. 40–43, Oct. 1999.

[45] E. M. Voumvoulakis, A. E. Gavoyiannis, and N. D. Hatziargyriou, "Decision trees for dynamic security assessment and load shedding scheme," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Jun. 2006, p. 7.

[46] E. M. Voumvoulakis and N. D. Hatziargyriou, "Decision trees-aided self-organized maps for corrective dynamic security," *IEEE Trans. Power Syst.*, vol. 23, no. 2, pp. 622–630, May 2008.

[47] K. S. Swarup and P. B. Corthis, "ANN approach assesses system security," *IEEE Comput. Appl. Power*, vol. 15, no. 3, pp. 32–38, Jul. 2002.

[48] R. Sunitha, R. S. Kumar, and A. T. Mathew, "Online static security assessment module using artificial neural networks," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4328–4335, Nov. 2013.

[49] Y. Du, F. Li, and C. Huang, "Applying deep convolutional neural network for fast security assessment with N-1 contingency," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2019, pp. 1–5.

[50] F. Li and Y. Du, "From AlphaGo to power system AI: What engineers can learn from solving the most complex board game," *IEEE Power Energy Mag.*, vol. 16, no. 2, pp. 76–84, Mar. 2018.

[51] A. N. Al-Masri, M. Z. A. A. Kadir, A. S. Al-Ogaili, and Y. Hoon, "Development of adaptive artificial neural network security assessment schema for Malaysian power grids," *IEEE Access*, vol. 7, pp. 180093–180105, 2019.

[52] A. N. Al-Masri, M. Z. A. A. Kadir, H. Hizam, and N. Mariun, "Simulation of an adaptive artificial neural network for power system security enhancement including control action," *Appl. Soft Comput.*, vol. 29, pp. 1–11, Apr. 2015.

[53] B. Wang, B. Fang, Y. Wang, H. Liu, and Y. Liu, "Power system transient stability assessment based on big data and the core vector machine," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2561–2570, Sep. 2016.

[54] S. Kalyani and K. S. Swarup, "Binary SVM approach for security assessment and classification in power systems," in *Proc. Annu. IEEE India Conf.*, Dec. 2009, pp. 1–4.

[55] M. Beiraghi and A. M. Ranjbar, "Online voltage security assessment based on wide-area measurements," *IEEE Trans. Power Del.*, vol. 28, no. 2, pp. 989–997, Apr. 2013.

[56] R. Diao, V. Vittal, and N. Logic, "Design of a real-time security assessment tool for situational awareness enhancement in modern power systems," *IEEE Trans. Power Syst.*, vol. 25, no. 2, pp. 957–965, May 2010.

[57] V. Vittal, "Application of phasor measurements for dynamic security assessment using decision trees," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2012, pp. 1–3.

[58] M. He, V. Vittal, and J. Zhang, "Online dynamic security assessment with missing PMU measurements: A data mining approach," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1969–1977, May 2013.

[59] R. Diao, K. Sun, V. Vittal, R. J. O'Keefe, M. R. Richardson, N. Bhatt, D. Stradford, and S. K. Sarawgi, "Decision tree-based online voltage security assessment using PMU measurements," *IEEE Trans. Power Syst.*, vol. 24, no. 2, pp. 832–839, May 2009.

[60] K. Sun, S. Likhate, V. Vittal, V. S. Kolluri, and S. Mandal, "An online dynamic security assessment scheme using phasor measurements and decision trees," *IEEE Trans. Power Syst.*, vol. 22, no. 4, pp. 1935–1943, Nov. 2007.

[61] X. Boyen and L. Wehenkel, "Automatic induction of fuzzy decision trees and its application to power system security assessment," *Fuzzy Sets Syst.*, vol. 102, no. 1, pp. 3–19, Feb. 1999.

[62] I. Kamwa, S. R. Samantaray, and G. Joos, "Development of rule-based classifiers for rapid stability assessment of wide-area post-disturbance records," *IEEE Trans. Power Syst.*, vol. 24, no. 1, pp. 258–270, Feb. 2009.

[63] Z. Nie, D. Yang, V. Centeno, and K. D. Jones, "A PMU-based voltage security assessment framework using Hoeffding-tree-based learning," in *Proc. 19th Int. Conf. Intell. Syst. Appl. Power Syst. (ISAP)*, Sep. 2017, pp. 1–6.

[64] P. Domingos and G. Hulten, "Mining high-speed data streams," in *Proc. 6th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Aug. 2000, pp. 71–80.

[65] I. Genc, R. Diao, V. Vittal, S. Kolluri, and S. Mandal, "Decision tree-based preventive and corrective control applications for dynamic security enhancement in power systems," *IEEE Trans. Power Syst.*, vol. 25, no. 3, pp. 1611–1619, Aug. 2010.

[66] E. S. Karapidakis and N. D. Hatziargyriou, "Online preventive dynamic security of isolated power systems using decision trees," *IEEE Trans. Power Syst.*, vol. 17, no. 2, pp. 297–304, May 2002.

[67] C. Liu, K. Sun, Z. H. Rather, Z. Chen, C. L. Bak, P. Thøgersen, and P. Lund, "A systematic approach for dynamic security assessment and the corresponding preventive control scheme based on decision trees," *IEEE Trans. Power Syst.*, vol. 29, no. 2, pp. 717–730, Mar. 2014.

[68] V. Krishnan, J. D. McCalley, S. Henry, and S. Issad, "Efficient database generation for decision tree based power system security assessment," *IEEE Trans. Power Syst.*, vol. 26, no. 4, pp. 2319–2327, Nov. 2011.

[69] J. L. Cremer, I. Konstantelos, and G. Strbac, "From optimization-based machine learning to interpretable security rules for operation," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 3826–3836, Sep. 2019.

[70] Z. H. Rather, C. Liu, Z. Chen, C. L. Bak, and P. Thøgersen, "Dynamic security assessment of Danish power system based on decision trees: Today and tomorrow," in *Proc. IEEE Grenoble Conf.*, Jun. 2013, pp. 1–6.

[71] M. Negnevitsky, N. Tomin, V. Kurbatsky, D. Panasetsky, A. Zhukov, and C. Rehtanz, "A random forest-based approach for voltage security monitoring in a power system," in *Proc. IEEE Eindhoven PowerTech*, Jun. 2015, pp. 1–6.

[72] W. D. Oliveira, J. P. A. Vieira, U. H. Bezerra, D. A. Martins, and B. D. G. Rodrigues, "Power system security assessment for multiple contingencies using multiway decision tree," *Electr. Power Syst. Res.*, vol. 148, pp. 264–272, Jul. 2017.

[73] M. He, J. Zhang, and V. Vittal, "Robust online dynamic security assessment using adaptive ensemble decision-tree learning," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4089–4098, Nov. 2013.

[74] Z. Li and W. Wu, "Phasor measurements-aided decision trees for power system security assessment," in *Proc. 2nd Int. Conf. Inf. Comput. Sci.*, vol. 1, 2009, pp. 358–361.

[75] J. A. Huang, A. Valette, M. Beaudoin, K. Morison, A. Moshref, M. Provencher, and J. Sun, "An intelligent system for advanced dynamic security assessment," in *Proc. Int. Conf. Power Syst. Technol.*, vol. 1, 2002, pp. 220–224.

[76] R. Tiako, D. Jayaweera, and S. Islam, "A class of intelligent algorithms for on-line dynamic security assessment of power systems," in *Proc. 20th Australas. Univ. Power Eng. Conf.*, Dec. 2010, pp. 1–6.

[77] S. Zhang, D. Zhang, J. Qiao, X. Wang, and Z. Zhang, "Preventive control for power system transient security based on XGBoost and DCOPF with consideration of model interpretability," *CSEE J. Power Energy Syst.*, vol. 7, no. 2, pp. 279–294, Mar. 2021.

[78] Y. Xu, Z. Y. Dong, J. H. Zhao, P. Zhang, and K. P. Wong, "A reliable intelligent system for real-time dynamic security assessment of power systems," *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1253–1263, Aug. 2012.

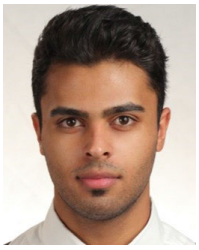
[79] Y. Xu, Z. Y. Dong, Z. Xu, K. Meng, and K. P. Wong, "An intelligent dynamic security assessment framework for power systems with wind power," *IEEE Trans. Ind. Informat.*, vol. 8, no. 4, pp. 995–1003, Nov. 2012.

[80] C. Ren, Y. Xu, Y. Zhang, and C. Hu, "A multiple randomized learning based ensemble model for power system dynamic security assessment," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2018, pp. 1–5.

[81] C. Cheng, G. Ma, Y. Zhang, M. Sun, F. Teng, H. Ding, and Y. Yuan, "A deep learning-based remaining useful life prediction approach for bearings," *IEEE/ASME Trans. Mechatronics*, vol. 25, no. 3, pp. 1243–1254, Jun. 2020.

[82] M. Sun, I. Konstantelos, and G. Strbac, "A deep learning-based feature extraction framework for system security assessment," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5007–5020, Sep. 2019.
[83] J. H. Arteaga, F. Hancharou, F. Thams, and S. Chatzivasileiadis, "Deep learning for power system security assessment," in *Proc. IEEE Milan PowerTech*, Jun. 2019, pp. 1–6.
[84] B. Tan, J. Yang, Y. Tang, S. Jiang, P. Xie, and W. Yuan, "A deep imbalanced learning framework for transient stability assessment of power system," *IEEE Access*, vol. 7, pp. 81759–81769, 2019.
[85] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 27, 2014, pp. 1–9.
[86] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," 2014, *arXiv:1412.6980*.
[87] J. M. Gimenez Alvarez and P. E. Mercado, "Online inference of the dynamic security level of power systems using fuzzy techniques," *IEEE Trans. Power Syst.*, vol. 22, no. 2, pp. 717–726, May 2007.
[88] Y. Xu, Z. Y. Dong, K. Meng, R. Zhang, and K. P. Wong, "Real-time transient stability assessment model using extreme learning machine," *IET Gener., Transmiss. Distrib.*, vol. 5, no. 3, pp. 314–322, Mar. 2011.
[89] Y. Xu, Z. Y. Dong, L. Guan, R. Zhang, K. P. Wong, and F. Luo, "Preventive dynamic security control of power systems based on pattern discovery technique," *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1236–1244, Aug. 2012.
[90] Y. Zhang, H. Zhang, L. Wang, and G. Hou, "Consistency analysis of SCADA data from field power systems," in *Proc. 10th Int. Conf. Adv. Power Syst. Control, Oper. Manage. (APSCOM)*, Nov. 2015, pp. 1–4.
[91] G. Ortiz, C. Rehtanz, and G. Colomé, "Monitoring of power system dynamics under incomplete PMU observability condition," *IET Gener., Transmiss. Distrib.*, vol. 15, no. 9, pp. 1435–1450, May 2021.
[92] K. Morison, L. Wang, and P. Kundur, "Power system security assessment," *IEEE Power Energy Mag.*, vol. 2, no. 5, pp. 30–39, Sep. 2004.
[93] J. Benesty, J. Chen, and Y. Huang, "On the importance of the Pearson correlation coefficient in noise reduction," *IEEE Trans. Audio, Speech, Language Process.*, vol. 16, no. 4, pp. 757–765, May 2008.
[94] S. Basu, K. Kumbier, J. B. Brown, and B. Yu, "Iterative random forests to discover predictive and stable high-order interactions," *Proc. Nat. Acad. Sci. USA*, vol. 115, no. 8, pp. 1943–1948, Feb. 2018.
[95] I. Xyngi, A. Ishchenko, M. Popov, and L. van der Sluis, "Transient stability analysis of a distribution network with distributed generators," *IEEE Trans. Power Syst.*, vol. 24, no. 2, pp. 1102–1104, May 2009.
[96] C. Ren, Y. Xu, B. Dai, and R. Zhang, "An integrated transfer learning method for power system dynamic security assessment of unlearned faults with missing data," *IEEE Trans. Power Syst.*, vol. 36, no. 5, pp. 4856–4859, Sep. 2021.
[97] C. Ren and Y. Xu, "Transfer learning-based power system online dynamic security assessment: Using one model to assess many unlearned faults," *IEEE Trans. Power Syst.*, vol. 35, no. 1, pp. 821–824, Jan. 2020.

ALIREZA MEHRZAD was born in Iran, in April 1993. He received the B.Sc. degree in power system electrical engineering from Islamic Azad University, Iran, in 2015, and the M.Sc. degree in power system electrical engineering from Birjand University, Birjand, Iran, in 2019. He is actively performing research in various fields of electrical engineering and power systems. His research interests include power system dynamics, security, demand response, applications of data-driven techniques in power systems, and distributed networks.



MILAD DARMIANI was born in Zahedan, Iran, in June 1994. He received the B.Sc. and M.Sc. degrees in electrical engineering from Birjand University, Birjand, Iran, in 2016 and 2019, respectively. He has working experience of two years with Sistan & Baluchestan Regional Electric Company, Zahedan. His research interests include power system dynamics, power system security, lightning and switching transients, demand response, renewable energy, and smart grids.

YASHAR MOUSAVI (Member, IEEE) received the Ph.D. degree from Glasgow Caledonian University, Glasgow, U.K., in 2023. He is a Senior Mechatronics CAE Engineer at American Axle & Manufacturing, Detroit, MI, USA. He majored in modeling, simulation, and analysis of combustion-based and electric vehicles' power transfer units, gear shift actuation systems, eLocker electric drive units, and full-vehicle driveline systems. He has carried out various projects for top-notch companies, such as General Motors, Stellantis, Ford, Mercedes Benz, and Volkswagen. He is also a Controls Integration Researcher with the Power and Renewable Energy Systems (PRES) Team, Glasgow Caledonian University. His research interests include vehicle dynamics modeling and analysis, power systems analysis, robust nonlinear control, fault-tolerant control, renewable energy, and robotic systems modeling and control.

MIADREZA SHAFIE-KHAH (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from Tarbiat Modares University, Tehran, Iran, and the Ph.D. degree in electromechanical engineering from the University of Beira Interior (UBI), Covilha, Portugal. He held a postdoctoral position with UBI and a postdoctoral position with the University of Salerno, Salerno, Italy. He is currently a Professor (tenure-track) with the University of Vaasa, Vaasa, Finland. His research interests include electricity markets, power system optimization, demand response, electric vehicles, price and renewable forecasting, and smart grids. He is a Top Scientist in the Research.com ranking in engineering and technology, and he has won five best paper awards at IEEE conferences. He is also an Editor of the IEEE TRANSACTIONS ON SUSTAINABLE ENERGY, an Associate Editor of the IEEE SYSTEMS JOURNAL, an Associate Editor of IEEE ACCESS, an Editor of the IEEE OPEN ACCESS JOURNAL OF POWER AND ENERGY, an Associate Editor of *IET RPG*, and the Guest Editor-in-Chief of the IEEE OPEN ACCESS JOURNAL OF POWER AND ENERGY.

MOHAMMADREZA AGHAMOHAMMADI was born in Iran, in August 1955. He received the B.Sc. degree from the Sharif University of Technology, in 1985, the M.Sc. degree from Manchester University (UMIST), in 1989, and the Ph.D. degree from Tohoku University, Japan, in 1994. He is a Professor with the Electrical Engineering Department and the Head of the Iran Dynamic Research Center. His research interests include the application of intelligent techniques and non-model-based approaches for dynamic security assessment and enhancement of power systems.