

# A hybrid CNN-LSTM approach for dynamic security assessment of power systems with GAN-based imbalanced database

Sasan Azad<sup>1</sup>, Mohammad Taghi Ameli<sup>1,\*</sup>, Hossein Ameli<sup>2</sup>, Goran Strbac<sup>2</sup>

<sup>1</sup> Department of Electrical Engineering, Abbaspour School of Engineering, Shahid Beheshti University, Tehran, Iran

<sup>2</sup> Control and Power Group, Imperial College London, London SW7 2AZ, UK

## ARTICLE INFO

### Article history:

Received: 11 November 2024

Revised: 3 December 2024

Accepted: 26 December 2024

### Keywords:

Dynamic security assessment  
Deep learning  
Generative adversarial network  
Convolutional neural network  
Long short-term memory  
Imbalanced data



**Copyright:** © 2024 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>)

## ABSTRACT

Recently, deep learning-based techniques in dynamic security assessment (DSA) have shown significant advances, enabling them to play a pivotal role in ensuring power systems' secure operation. However, imbalanced samples are a fundamental challenge for effective training of data-driven methods. In the DSA problem, especially in real-world power systems, the database is usually imbalanced and the number of secure cases is more than the number of insecure cases. This imbalance can lead to loss of fit and generalization in insecure cases since the DSA model tends to focus too much on secure cases. In past studies, methods based on linear interpolators have been used, which cannot satisfy the power system's physical characteristics. This paper addresses the data imbalance in DSA by using generative adversarial networks (GANs) to generate synthetic data resembling the original data. After addressing the data imbalance, a hybrid model consisting of a convolutional neural network (CNN) and long short-term memory (LSTM) is developed in an integrated framework for DSA. The proposed model was implemented and tested on the IEEE 39 bus system. The test results show that solving the data imbalance problem has improved the proposed DSA model's performance.

## Abbreviations

DSA	Dynamic security assessment	DT	Decision tree
DL	Deep learning	ELM	Extreme learning machine
GAN	Generative adversarial network	SVM	Support vector machine
CNN	Convolutional neural network	RVFL	Random vector functional link network
LSTM	Long short-term memory	DT	Decision tree
WAMS	Wide-Area Measurement Systems	ELM	Extreme learning machine
PMU	Phasor measurement unit	RNN	Recurrent Neural Network
OC	Operating condition	DNN	Deep neural network
ANN	Artificial neural network	DT	Decision tree
SVM	Support vector machine	ELM	Extreme learning machine
RVFL	Random vector functional link network	CCT	Critical clearing time


## 1. Introduction

As the load increases and the stability margin of power systems decreases, the system may be operated under stress. In this situation, dynamic security assessment is necessary to prevent system instability. Violation of

dynamic security can cause irreparable accidents, including cascading failures and, of course, massive outages. As a result, it is necessary to pay attention to the system's dynamic security evaluation for its stable operation [1]. In recent years, the DSA of power systems

\* Corresponding author

E-mail address: [m\\_ameli@sbu.ac.ir](mailto:m_ameli@sbu.ac.ir)

 <https://orcid.org/0000-0002-8815-1596>

<http://dx.doi.org/10.48308/ijrtei.2024.237543.1062>

has required time domain simulations and complex calculations. These complex methods are known as traditional methods [2]. With the widespread installation of phasor measurement units (PMU) in power systems and the launch of wide-area measurement systems (WAMS), large amounts of data with high quality and resolution are available from the system. The existence of high-quality data rich in valuable information has made it possible to use data-based approaches in various power system applications [3].

Data-driven DSA approximates the system's dynamic response to various faults. It is less complicated than conventional methods and suitable for online applications [4]. According to this conditions, the operator can evaluate the dynamic security quickly and close to zero. Therefore, the margin of static stability during system operation can be reduced. Therefore, the operator can maximize the system infrastructure's use by reducing the static stability margin[5]. The idea behind data-driven methods is to train a model offline and use that model in an online application. To train an adequate model, an information-rich training database must be built for various operating conditions and contingency fault sets [6]. The studies conducted in the field of data-driven DSA have provided satisfactory results [7]. The presented data-driven methods can be divided into two categories: shallow methods and deep learning(DL)-based methods. Some of the used shallow methods are artificial neural networks (ANN) [5,2,8], decision trees (DTs) [9,10], and extreme learning machines (ELMs) [11], support vector machines (SVM) [12], and functional random vector networks (RVFL) [13].

In the meantime, since DL-based approaches have a deeper structure, they have obtained better results for DSA [14]. In [15], a DL-based approach for DSA is presented by providing an index that quantifies adversarial attacks. In [16], a data-driven DSA model is given by combining transfer learning(DL), deep neural networks (DNN), and long short-term memory(LSTM) models. In [15], a DL-based approach for DSA is presented by providing an index that quantifies adversarial attacks. In [16], a data-driven DSA model is given by combining transfer learning(DL), deep neural networks (DNN), and long short-term memory(LSTM) models. Also, in [17], a method for transient security evaluation is presented by combining convolutional neural networks(CNN) and feature selection techniques.

The presented methods have provided satisfactory results so far. However, when implemented in real-world power systems, these methods face the problem of imbalance in the training database. Since the imbalance in the database can cause the performance of data-based models to drop, researchers must pay attention to this issue. According to the stated challenge, this research uses a Generative adversarial network(GAN) algorithm to generate synthetic data to solve the imbalanced database challenge. The GAN is currently one of the best unsupervised deep learning methods and has been used in a wide range of applications from the creation of images to the creation of audio and text [18]. To address this issue, this study introduces a resampling technique

designed to create synthetic data resembling the minority class present in an imbalanced database. By specifying the rare class, the GAN can resolve overfitting and class overlap problems. The final database consists of the synthetic data generated by the GAN and the original imbalanced data. Finally, the DSA model based on a hybrid CNN-LSTM is trained using the final database.

## 2. Deep Learning Models for DSA

### 2.1. Generative Adversarial Network

GAN represents a form of unsupervised ML algorithm with the capacity to produce exceedingly authentic features and patterns directly derived from the training dataset, all while circumventing the necessity for explicit models or pre-existing training procedures. The GAN methodology encompasses two complex deep neural networks: a generator and a discriminator. These networks undergo training through adversarial learning techniques, aiming to refine and enhance the generation of progressively authentic content in each successive iteration. The generator functions by synthesizing fresh samples through the reception of random noise as input, subsequently adjusting them with the distribution characteristics of actual data samples. In contrast, the discriminator's role entails the discrimination of data instances, accompanied by the computation of probabilities associated with their origin, which may either stem from the original dataset or originate from the generator [19]. A visual representation of the GAN network's structure is depicted in Fig. 1 for reference.

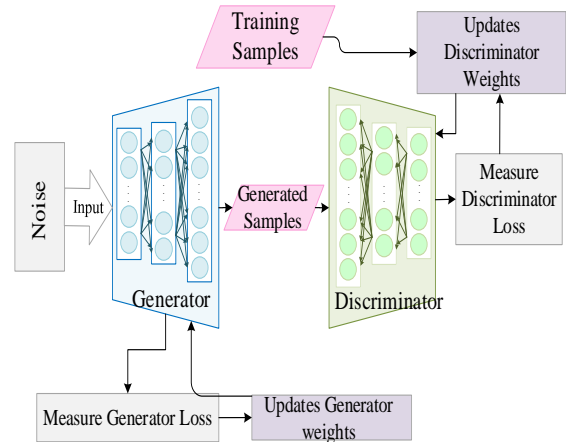


Fig. 1. Structure of GAN network

- Generator: Consider  $p_g$  to represent the actual distribution of observable features within dataset  $x$ . In this context, it is possible to establish a prior distribution for the input noise vector  $z$ , denoted as  $z \sim p_z(z)$ , which can be efficiently utilized for sampling purposes. The objective is to discover a function  $G$ , denoted as  $G(z, \theta_g)$ , that follows the distribution  $p_g(x)$  after undergoing a transformation. Here,  $G$  is defined as a differentiable function and is realized through a multilayer perceptron [20].
- Discriminator: We shall denote a secondary multilayer perceptron as  $D(x, \theta_d)$ , assigned to generate a single scalar output. More precisely, the function  $D(x)$  is employed to quantify the

likelihood that the input data point  $x$  originates from the generated dataset rather than the original data distribution,  $p_g$ . In light of this premise, the goal is to enhance the probability of precisely distinguishing between input data originating from actual and generated sources, denoted as  $\mathbb{E}[D(x)]$  and  $\mathbb{E}[D(G(z))]$ , respectively.

GANs training process can be divided into two separate phases. The Discriminator network is updated in the first phase while keeping the Generator parameters fixed. Subsequently, the Generator network is updated with fixed Discriminator parameters in the second phase. In alignment with the defined goals for both the Generator and Discriminator networks, the neural network weights necessitate adjustment through the optimization of specific loss functions. To be precise, the loss functions for the Discriminator and Generator are individually formulated as depicted below [20]:

$$\max_D V(D, G) = \mathbb{E}_{x \sim p_{data}(x)} [\log D(x)] + \mathbb{E}_{z \sim p_z(z)} [\log(1 - D(G(z)))] \quad (1)$$

$$\max_G V(D, G) = \mathbb{E}_{z \sim p_z(z)} [\log(D(G(z)))] \quad (2)$$

Here, Eq. (5) is equivalent to Eq. (6) demonstrated as follows:

$$\max_G V(D, G) = \mathbb{E}_{z \sim p_z(z)} [\log(1 - D(G(z)))] \quad (3)$$

Ultimately, we merge Eq. (1) with Eq. (3) to construct a two-player iterative minimax game represented by the value function  $V(G, D)$ :

$$\min_G \max_D V(D, G) = \mathbb{E}_{x \sim p_{data}(x)} [\log D(x)] + \mathbb{E}_{z \sim p_z(z)} [\log(1 - D(G(z)))] \quad (4)$$

This function aims to create stable fixed states in both the generator (referred to as G) and the discriminator (referred to as D). Moreover, it produces enhanced gradients, especially in the early stages of the learning process. In cases where G is ineffective, the function allows D to confidently identify and reject samples because they noticeably differ from the training data. This paper aims to utilize the data generation methods of the GAN model to produce datasets with significantly imbalanced classes. The datasets will be balanced before being used for classification.

## 2.2. Principles of Long Short-Term Memory

Since DL approaches have provided satisfactory results, they have gained high acceptance. Among them, methods based on recurrent neural networks (RNN) are known as useful methods for time series data and sequential data. However, these methods are prone to gradient reduction. Therefore, this paper uses LSTM to deal with the gradient explosion problem[21].

In LSTM, "cell state" is known as the fundamental concept. By processing the input data ( $x_t$ ) at each step, the cell state ( $c_t$ ) is updated, and a time-dependent feature

vector ( $h_t$ ) is generated. In LSTM, the flow of information is moderated by three gates: the input gate ( $i_t$ ), the forgetting gate ( $f_t$ ), and the output gate ( $o_t$ ). In this situation, a decision is made regarding the preservation of information according to the forgetting gate's performance. A forgetting gate produces a number between 0 and 1. If this number is close to 1, the information is kept; if it is close to 0, it is deleted. This is done using the sigmoid activation function ( $\sigma$ ). Subsequently, the input gate selects the new information from the present time step to update the status of the cell with  $g_t$ . And eventually, the output gate chooses the amount of data that ought to be transmitted from an earlier stage to the next one [22]. The LSTM equations are as follows:

$$f_t = \sigma(W_{if}x_t + W_{hf}h_{t-1} + b_f) \quad (5)$$

$$i_t = \sigma(W_{ii}x_t + W_{hi}h_{t-1} + b_i) \quad (6)$$

$$g_t = \sigma(W_{ig}x_t + W_{hg}h_{t-1} + b_g) \quad (7)$$

$$o_t = \sigma(W_{io}x_t + W_{ho}h_{t-1} + b_o) \quad (8)$$

$$c_t = f_t c_{t-1} + g_t c_t \quad (9)$$

$$h_t = o_t \tanh(c_t) \quad (10)$$

LSTM weights for each gate are symbolized as  $W_{if}$ ,  $W_{hf}$ ,  $W_{ii}$ ,  $W_{hi}$ ,  $W_{ig}$ ,  $W_{hg}$ ,  $W_{io}$ , and  $W_{ho}$ . Additionally, the biases for each cell are  $b_f$ ,  $b_i$ ,  $b_g$ , and  $b_o$ . The architecture of an LSTM and its chain representation are shown in Fig. 2.

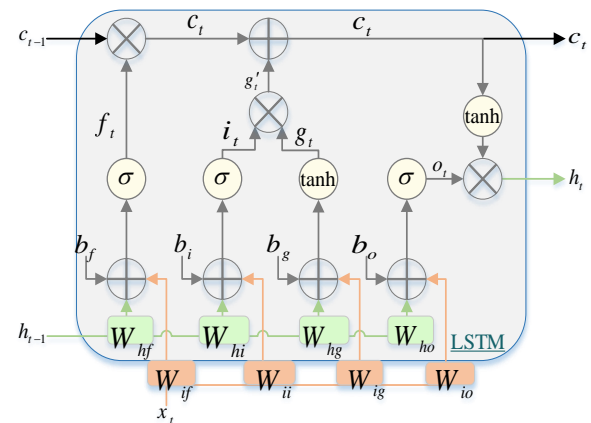


Fig. 2. Block diagram of LSTM

## 2.3. Principle of Convolutional Neural Networks

Convolutional Neural Networks (CNNs) are widely used in computer vision and imaging as one of the most robust Deep Learning models. Today, due to their exceptional performance in tackling complex problems, researchers and professionals across various fields leverage CNNs. CNN architectures typically consist of two stages: feature extraction and classification. The following briefly describes the different layers utilized in CNN architecture:

a) Convolutional layers: The convolutional layer comprises feature detectors or filters and generates feature maps. This layer convolves input data with filters to produce feature maps. Feature detectors slide over the input, computing dot products at each position to create stacked activation maps [23].

b) Pooling layers: The pooling layer receives feature maps from the convolutional layer. Its role is to reduce feature map dimensionality while retaining essential features. Pooling can be performed using average or maximum methods. Utilizing the pooling layer helps prevent overfitting and enhances model performance [23].

c) Batch Normalization Layer: Batch normalization fixes the means and variances of each layer's input [24]. It has been demonstrated in various experiments to accelerate training, enhance efficiency, and stabilize deep neural networks. Despite its proven effectiveness, the underlying reasons for its efficiency remain unclear [25]. Considering the  $p$ -dimensional input to a BN layer,  $x = (x_1, x_2, \dots, x_j)$  the BN layer is transformed as follows:

$$\tilde{x}_j = \frac{x_j - E[x_j]}{\sqrt{\text{Var}[x_j]}} \quad (11)$$

$$y_j = \gamma_j \tilde{x}_j + \beta_j$$

Where  $y_j$  is the output of one neuron response, the parameters  $\gamma_j$  and  $\beta_j$  refer to the scale and shift parameters, respectively.

d) Dropout Layer: Dropout is a technique used to combat overfitting in neural networks by randomly deactivating units during training [26]. Despite its simplicity, this method is highly effective and efficient.

e) Fully connected layers: Fully Connected Layers are part of feed-forward neural networks. These layers typically constitute the final layers in CNN-based models and are responsible for carrying out the ultimate classification tasks [23]. The output from the initial layers in the CNN architecture, which handle feature extraction, is passed to the fully connected layers after being flattened.

### 3. Proposed DSA Method

Different parts of the GAN-based proposed approach to managing imbalanced data can be seen in Fig. 3. Subsequent to the normalization of the dataset, a partition was implemented, allocating 75% of the data for the training phase and reserving 25% for testing purposes. The training database is structured after an in-depth examination of the sparsely represented training data class by applying GANs and resampling techniques. The proposed approach obtains the database by combining the original imbalanced database and the generated synthetic data. Finally, the obtained balanced database helps build the proposed CNN-LSTM approach.

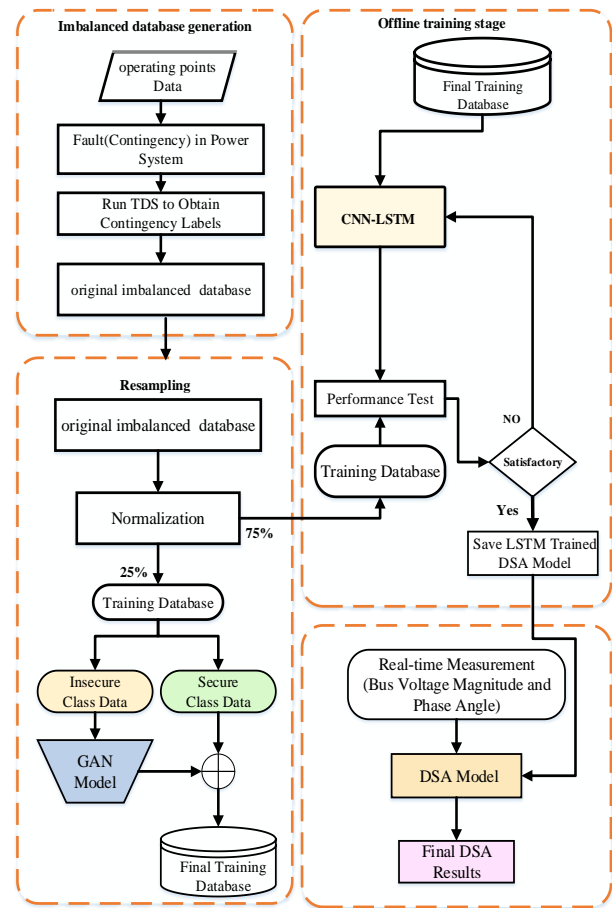


Fig. 3. Flowchart of the proposed method

#### 3.1. Imbalanced Database Generation

To train the DSA model, a database must first be created. This database consists of a combination of operating points before the fault and the corresponding labels after the fault. The input data to the model or pre-fault data are voltage ( $V$ ) and phase angles ( $\theta$ ). These data are collected directly through PMUs installed on buses with generators. The database formulation is as follows

$$X_{original} = \{x_1; x_2; \dots; x_k; \dots; x_N\}, k \in [1, n] \quad (12)$$

$$x_k = \{V, \theta\}, V \in \mathbb{R}^g, \theta \in \mathbb{R}^g \quad (13)$$

$g$  shows the number of generators and  $n$  shows the number of OCs.  $Y_{original}$  also indicates the label of OCs.

$$Y_{original} = \{y_1; y_2; \dots; y_k; \dots; y_N\}, k \in [1, n] \quad (14)$$

In this work, the system is considered unstable if the rotor angle difference of at least two generators exceeds 180 degrees after the fault [14].

#### 3.2. Offline Training Stage

In this stage, the database created in the previous step is split into two parts: training and testing, with a ratio of 4:1. The training database will be utilized to train the hybrid CNN-LSTM model. This paper introduces a hybrid CNN-LSTM model for DSA using the training database. The architecture of the proposed hybrid CNN-LSTM model is depicted in Fig. 4.

The hybrid CNN-LSTM model in this study comprises two convolutional layers, two max-pooling

layers, the LSTM layer, two fully connected layer for feature interpretation, and the output layer. The convolutional layers are built using kernels of size 3, with each activation block employing the Rectified Linear Unit (ReLU) function. The pooling layer in the CNN structure utilizes the maximum value function, with a pooling size and strides of 2 and 1, respectively. Batch normalization is incorporated to enhance learning convergence and domain adaptation. Dropout is applied before the LSTM layer to mitigate overfitting. ReLU activation is used for the dense layers, while softmax is employed in the output layer for classification.

$$y = \text{softmax}(w_d s + b_d) \quad (15)$$

In Equation (15),  $s$  denotes the input of the softmax layer. Additionally,  $w_d$  and  $b_d$  represent the weight and bias matrices that the assessment model must learn during training.

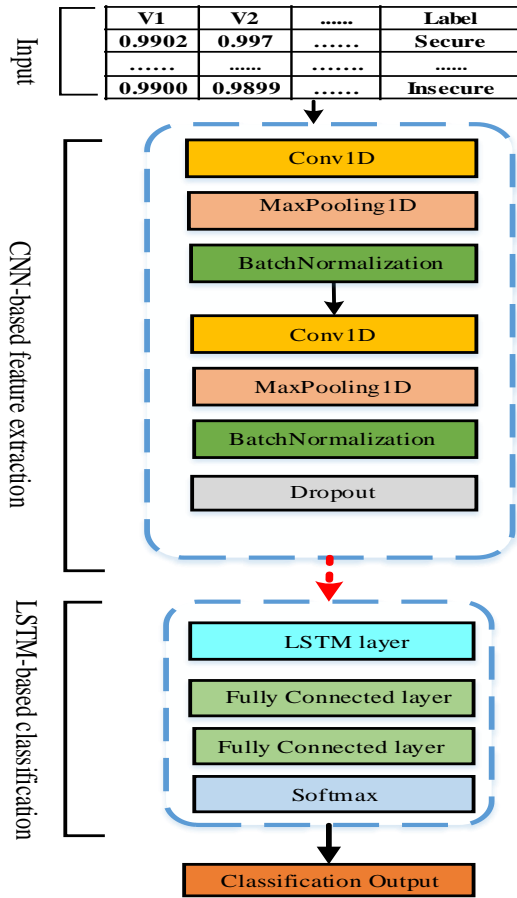


Fig. 4. Structure of proposed model

In the offline training stage, the CNN-LSTM-based assessment model is trained to minimize the discrepancy between the model predictions and the actual states, and the learning parameters are obtained. To achieve this objective, a loss function and an optimization algorithm for the learning parameters are essential. In this case, the model predictions and actual states are compared through the loss function, and the optimization algorithm seeks to reduce the loss function by iteratively updating the learning parameters. The cross-entropy (CE) function has demonstrated excellent performance in classification tasks and has been extensively employed in various research [27]. In this work, CE has been utilized as a loss function, and Adam's algorithm has been employed to

optimize it. This algorithm is widely used in DL and produces excellent generalization results relatively quickly in the DSA classification problem.

### 3.3. Online Application

Real-time data is gathered using PMUs during the online application phase. Once these measurements are obtained, they are input into the assessment model, which has previously acquired its optimal parameters through offline training. Subsequently, the DSA result for a system can be promptly determined. If the assessment outcome signals that the system is at risk of losing stability, immediate corrective control actions must be initiated to avert instability. Conversely, if the assessment model indicates that the system remains secure, it continues monitoring its stability status.

### 3.4. Evaluation Indexes

With the widespread installation of PMUs, high-quality and high-resolution data are available to the operator, increasing the accuracy of DSA models [28, 29]. Meanwhile, dealing with false positives is necessary to train a suitable model [30]. In past studies, less attention has been paid to Type I errors, which involve misclassifying an insecure situation as secure. The models presented so far have primarily focused on increasing the accuracy [31]. In this study, Type I error is used for evaluation in addition to accuracy, recall, and precision criteria. Table 1 shows the confusion matrix with variables F11, F00, F10 and F01. The following indicators are used to evaluate the proposal model.

Table 1. Confusion matrix for DSA

Actual	Prediction	
	Insecure	Secure
Insecure	F <sub>00</sub>	F <sub>01</sub>
Secure	F <sub>10</sub>	F <sub>11</sub>

$$\text{Precision} = \frac{F_{00}}{F_{00} + F_{01}} \quad (16)$$

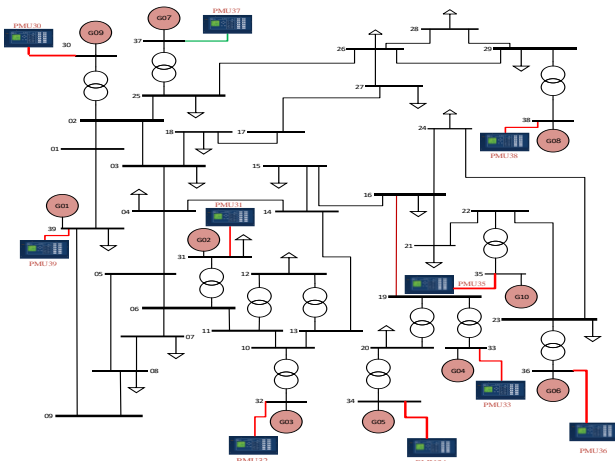
$$\text{Recall} = \frac{F_{00}}{F_{00} + F_{10}} \quad (17)$$

$$\text{Accuracy} = \frac{F_{00} + F_{11}}{F_{00} + F_{01} + F_{10} + F_{11}} \quad (18)$$

$$\text{Type I error rate} = \frac{F_{01}}{F_{00} + F_{01}} \quad (19)$$

## 4. Simulation results

This section examines the proposed model's performance in DSA and data augmentation using the IEEE 39 bus system. Fig. 5 illustrates the system diagram, comprising 10 generators, 46 transmission lines, and 39 buses. In this work, PMUs are installed on buses equipped with generators. The hyperparameters for the CNN-LSTM model is comprehensively detailed in Table 2. Furthermore, the proposed model is compared against other established models, including CNN [14], LSTM [32], DT [33], and RF [31]. The proposed scheme will be implemented using the Digsilent Power Factory and Python platforms.



**Fig. 5. The IEEE 39-bus test system**

**Table 2. hyper-parameters**

Layers	Hyper-parameters
Convolution Layer	Number of kernels:32 Size of kernels: 3 Strides: 1
Pooling Layer (MaxPooling)	Size of pooling:2 Strides: 1
Batch Normalization Layer	-
Convolution Layer	Number of kernels:64 Size of kernels: 3 Strides: 1
Pooling Layer (MaxPooling)	Size of pooling:2 Strides: 1
Batch Normalization	-
Dropout	dropout rate: 0.1
LSTM	256 cells
Dense	128 units
Dense	32 units
Output Layer (Dense)	2 classifications

#### 4.1. Database Generation

The proposed method has been implemented using simulations on the IEEE 39 bus system. For this purpose, different operating points have been randomly generated. Random operating points were obtained by sampling from 0.7 to 1.25 times the base load value. By doing this, many operating points are obtained and labeled as secure and insecure by simulating the time domain and based on contingency faults. This paper considers three-phase faults with interregional corridor trips as contingencies. The contingencies considered in this study are 8 faults with inter-area corridor trips. The faults settings are shown in Table 3. In this section, a total of 5000 samples were generated through these simulations. Finally, a GAN model is trained with insecure data to balance the database and then generates artificial samples. Doing this creates a database containing 7,500 samples that allow for proper training of the DSA model. For model training,

80% of the operating points are randomly selected, and the remaining 20% are used for model testing.

**Table 3. Contingency faults**

Fault Number	Fault setting	Duration(s)
F1	Fault bus 3, Trip 3-4	0.15
F2	Fault bus 4, Trip 3-4	0.15
F3	Fault bus 4, Trip 4-14	0.2
F4	Fault bus 14, Trip 4-14	0.2

F5	Fault bus 2, Trip 2-3	0.1
F6	Fault bus 3, Trip 2-3	0.1
F7	Fault bus 6, Trip 6-11	0.15
F8	Fault bus 11, Trip 6-11	0.15
F9	Fault bus 22, Trip 22-23	0.1
F10	Fault bus 23, Trip 22-23	0.1

#### 4.2. Effect of Data Augmentation on Model Performance

Table 4 presents the test results of the proposed method, both before and after data augmentation. This analysis indicates that the DSA model exhibits superior performance when trained with the resampling data compared to the original database.

**Table 4. Performance of the proposed model before and after resampling**

Proposed method	Accuracy	Recall	Precision	Type I error rate
After resampling	99.41%	99.45%	98.99%	1%
before resampling	94.34%	95.14%	92.94%	7.15%

Hence, addressing the class imbalance issue to enhance the performance of the DSA model warrants significant consideration. The findings reveal a noteworthy improvement in the DSA model's accuracy, with an increase of 5.07%, which can be highly valuable in preventing power system instability. Furthermore, recall and precision metrics exhibit notable enhancements of 4.31% and 6.05%, respectively. In DSA, system operators' precise identification of insecure operational points assumes paramount significance. Consequently, one of the pivotal aspects in the field of DSA is quantifying F01 cases, signifying instances where insecure states are erroneously classified as secure. Such misclassifications have the potential to cause cascading failures or widespread outages. In light of this, this paper employs the Type I error rate criterion to examine this concern. The results evince a reduction of 6.15% in the Type I error rate of the proposed model with the incorporation of resampling techniques.

#### 4.3. Comparing Performance of Proposed Model with Other Classifiers

In this section, a comprehensive comparison is made between the proposed model and other classifiers with balanced data. Using accuracy, recall, precision and type I error evaluation indices, the proposed model was reasonably evaluated compared to CNN [14], LSTM [31], DT[32] and RF[30]. All tests were performed 5 times with different random seeds to provide a valid comparison of other classifiers. Table 5 shows the accuracy results of different algorithms.

**Table 5. Comparison of results of proposed model with existing methods**

Classifier	Accuracy	Recall	Precision	Type I error rate
Proposed	99.41	99.45	98.99	1.00
CNN[14]	99.23	99.25	98.69	1.31
LSTM[31]	99.12	99.12	98.54	1.45
DT[32]	97.20	97.06	95.49	4.51
RF[30]	97.95	97.97	96.58	3.42

Table 5 shows that the proposed model has the highest accuracy and CNN and LSTM have better accuracy than DT and SVM. This shows that DL-based methods are superior. Table 5 shows that the proposed model has the highest accuracy and CNN and LSTM have better accuracy than DT and SVM. This indicates that DL-based methods are superior. The proposed model's recall value is 99.45%. Table 5 shows that the proposed model's recall value is higher than that of DT and SVM models, as well as CNN and LSTM models. Also, the precision and Type I error rate for the proposed model are 98.99% and 1%, respectively. This is better performance than CNN, LSTM, DT and SVM. The results confirm that the proposed model based on GCN performs better than CNN, LSTM, DT and SVM.

#### 4.4. sensitivity analysis with noise data

Although PMUs are precise measuring devices, the data they provide may contain noise and errors [34]. The IEEE standard C37.118-2005 stipulates that the Total Vector Error (TVE) of PMUs should be less than 1% [35]. TVE represents the discrepancy between the signals measured by the PMUs and the actual applied signals. This paper explores the impact of PMU noise and measurement error as follows:

Scenario 1: NO noisy data.

Scenario 2: Test data is noisy.

Scenario 3: Training and testing data are noisy.

The test results for the described scenarios are presented in Table. 6. These results demonstrate that noisy data diminishes the accuracy of the proposed models but remains within an acceptable range for DSA.

**Table 6.** Performance of proposed model for noisy data

Classifier	Accuracy(%)		
	Scenario 1	Scenario 2	Scenario 3
Proposed method	99.41	95.85	97.68

#### 4.5. Performance Testing with Different Penetration Levels of Renewable Energy Sources

It is imperative to note that as a result of the increased penetration of renewable energy sources (RESs) in power systems, the dynamic characteristics of those systems have become more complex. There has been little research into the integration of these resources into the power system and how this impacts ML-based DSA techniques in the past. Therefore, further studies on the effect of different levels of RES penetration on ML-based DSA methods are necessary. There is a major question to be answered regarding the effectiveness of ML-based DSA methods in power systems incorporating

#### References

- [1] Mollaiee, A., Ameli, M. T., Azad, S., Nazari-Heris, M., & Asadi, S. (2023). Data-driven power system security assessment using high content database during the COVID-19 pandemic. *International Journal of Electrical Power & Energy Systems*, 150, 109077.
- [2] Liu, S., Liu, L., Fan, Y., Zhang, L., Huang, Y., Zhang, T., ... & Mao, D. (2020). An integrated scheme for online dynamic security assessment based on partial mutual information and iterated random forest. *IEEE Transactions on Smart Grid*, 11(4), 3606-3619.

RESs. In this study, we investigate the performance of the proposed method at different RES penetration levels. Table 7 shows the proposed model's performance accuracy results for different RES penetration levels.

**Table 7.** Accuracy of proposed model under different penetration levels of RESs

Penetrations rates (%)	Accuracy(%)
0	99.41
15	99.52
30	99.58

Table 7 shows that with the increase of the penetration coefficient of RES, not only the performance accuracy of the proposed model remained constant, but also improved. In a power system with less inertia, which may exhibit more linear characteristics, ML-based methods may perform better due to clearer boundaries separating secure and insecure points. This makes data-based DSA methods learn security assessment rules better in offline training and be more effective in online applications. It is necessary to explain that the full investigation of the influence of RESs penetration requires more studies, which are outside the focus of this study. The impact of distribution systems and RES on power systems is one topic that should be considered in future works. [36] proves that the distribution system reduces the power system's stability margin.

#### 5. Conclusion

Despite the satisfactory results of data-driven DSA methods, these methods face the challenge of an imbalanced database. This paper introduces an innovative model to mitigate the adverse effects of database imbalance on power system DSA. Based on the GAN model, the proposed model balances the database by resampling. This balancing process elevates the proposed model's accuracy from 94.34% to 99.41%. Also, the test results of the proposed model in noisy environments confirm its good robustness. Furthermore, the results show that the integration of RESs into the power system has increased the performance accuracy of data-driven DSA methods. This improvement in performance accuracy can be attributed to the more distinct boundaries between secure and insecure operating conditions in power systems with lower inertia, which facilitates the offline extraction of security rules for online assessments using machine learning techniques. Since generating an extensive database is difficult, time-consuming, and expensive, and DL-based models require a large database for effective training, the authors consider training a model with a small and unbalanced database for future work.

- [3] Mollaiee, A., Ameli, M. T., & Azad, S. (2022). Novel continuous learning scheme for online static security assessment based on the weather-dependent security index. *IET Generation, Transmission & Distribution*, 16(18), 3684-3705.

- [4] Sun, M., Konstantelos, I., & Strbac, G. (2018). A deep learning-based feature extraction framework for system security assessment. *IEEE transactions on smart grid*, 10(5), 5007-5020.

- [5] Bellizio, F., Cremer, J. L., & Strbac, G. (2022). Machine-learned security assessment for changing system topologies.

- International Journal of Electrical Power & Energy Systems, 134, 107380.
- [6] Konstantelos, I., Jamgotchian, G., Tindemans, S. H., Duchesne, P., Cole, S., Merckx, C., ... & Panciatici, P. (2016). Implementation of a massively parallel dynamic security assessment platform for large-scale grids. *IEEE Transactions on Smart Grid*, 8(3), 1417-1426.
- [7] Ren, C., Xu, Y., Dai, B., & Zhang, R. (2021). An integrated transfer learning method for power system dynamic security assessment of unlearned faults with missing data. *IEEE Transactions on Power Systems*, 36(5), 4856-4859.
- [8] Bellizio, F., Bugaje, A. A. B., Cremer, J. L., & Strbac, G. (2022). Verifying machine learning conclusions for securing low inertia systems. *Sustainable Energy, Grids and Networks*, 30, 100656.
- [9] Zhang, T., Sun, M., Cremer, J. L., Zhang, N., Strbac, G., & Kang, C. (2021). A confidence-aware machine learning framework for dynamic security assessment. *IEEE Transactions on Power Systems*, 36(5), 3907-3920.
- [10] Chen, Z., Ren, C., Xu, Y., Dong, Z. Y., & Li, Q. (2024). Data-driven power system dynamic security assessment under adversarial attacks: Risk warning based interpretation analysis and mitigation. *IET Energy Systems Integration*, 6(1), 62-72.
- [11] Singh, M., & Chauhan, S. (2023). A hybrid-extreme learning machine based ensemble method for online dynamic security assessment of power systems. *Electric Power Systems Research*, 214, 108923.
- [12] Lin, Y., & Wang, X. (2022). A Data-Driven Scheme Based on Sparse Projection Oblique Randomer Forests for Real-Time Dynamic Security Assessment. *IEEE Access*, 10, 79469-79479.
- [13] Zhang, Y., Xu, Y., & Dong, Z. Y. (2017). Robust classification model for PMU-based online power system DSA with missing data. *IET Generation, Transmission & Distribution*, 11(18), 4484-4491.
- [14] Azad, S., & Ameli, M. T. (2024). A domain adaptation-based convolutional neural network incorporating data augmentation for power system dynamic security assessment. *The Journal of Engineering*, 2024(7), e12400.
- [15] Ren, C., & Xu, Y. (2022). Robustness verification for machine-learning-based power system dynamic security assessment models under adversarial examples. *IEEE Transactions on Control of Network Systems*, 9(4), 1645-1654.
- [16] Liu, S., Liu, L., Yang, N., Mao, D., Zhang, L., Cheng, J., ... & Shi, R. (2021). A data-driven approach for online dynamic security assessment with spatial-temporal dynamic visualization using random bits forest. *International Journal of Electrical Power & Energy Systems*, 124, 106316.
- [17] Pournabi, M., Mohammadi, M., Afrasiabi, S., & Setoodeh, P. (2022). Power system transient security assessment based on deep learning considering partial observability. *Electric Power Systems Research*, 205, 107736.
- [18] Zhu, L., Chen, Y., Ghamisi, P., & Benediktsson, J. A. (2018). Generative adversarial networks for hyperspectral image classification. *IEEE Transactions on Geoscience and Remote Sensing*, 56(9), 5046-5063.
- [19] Habibi, O., Chemmakha, M., & Lazaar, M. (2023). Imbalanced tabular data modelization using CTGAN and machine learning to improve IoT Botnet attacks detection. *Engineering Applications of Artificial Intelligence*, 118, 105669.
- [20] Ren, C., & Xu, Y. (2019). A fully data-driven method based on generative adversarial networks for power system dynamic security assessment with missing data. *IEEE Transactions on Power Systems*, 34(6), 5044-5052.
- [21] Elsayed, N., ElSayed, Z., & Maida, A. S. (2023). LiteLSTM Architecture Based on Weights Sharing for Recurrent Neural Networks. *arXiv preprint arXiv:2301.04794*.
- [22] Shadi, M. R., Ameli, M. T., & Azad, S. (2022). A real-time hierarchical framework for fault detection, classification, and location in power systems using PMUs data and deep learning. *International Journal of Electrical Power & Energy Systems*, 134, 107399.
- [23] Ramirez-Gonzalez, M., Sevilla, F. R. S., Korba, P., & Castellanos-Bustamante, R. (2022). Convolutional neural nets with hyperparameter optimization and feature importance for power system static security assessment. *Electric Power Systems Research*, 211, 108203.
- [24] Ioffe, S., & Szegedy, C. (2015, June). Batch normalization: Accelerating deep network training by reducing internal covariate shift. In *International conference on machine learning* (pp. 448-456). pmlr.
- [25] Marani, A., & Nehdi, M. L. (2022). Predicting shear strength of FRP-reinforced concrete beams using novel synthetic data driven deep learning. *Engineering Structures*, 257, 114083.
- [26] Shi, Z., Yao, W., Zeng, L., Wen, J., Fang, J., Ai, X., & Wen, J. (2020). Convolutional neural network-based power system transient stability assessment and instability mode prediction. *Applied Energy*, 263, 114586.
- [27] Tapia, E. A., Colomé, D. G., & Rueda Torres, J. L. (2022). Recurrent Convolutional Neural Network-Based Assessment of Power System Transient Stability and Short-Term Voltage Stability. *Energies*, 15(23), 9240.
- [28] Azad, S., Pourmoradi, N., Amiri, M. M., & Bajaj, M. (2024). Deep Learning for Dynamic Security Assessment of Power Systems with Adaptive Synthetic Sampling-Based Imbalanced Database: A Case Study. In *Artificial Intelligence in the Operation and Control of Digitalized Power Systems* (pp. 381-397). Cham: Springer Nature Switzerland.
- [29] Mollaiee, A., Azad, S., Ameli, M. T., & Nazari-Heris, M. (2021). Voltage stability assessment in power grids using novel machine learning-based methods. *Application of machine learning and deep learning methods to power system problems*, 177-210.
- [30] Aghdam, T. S., Karegar, H. K., & Zeineldin, H. H. (2017). Transient stability constrained protection coordination for distribution systems with DG. *IEEE Transactions on Smart Grid*, 9(6), 5733-5741.
- [31] Liu, S., Mao, D., Zhang, T., Tang, F., Yang, N., Xue, T., ... & Shi, R. (2021). An integrated scheme for dynamic security assessment considering misclassification constraint based on umbrella Neyman-Pearson classifiers. *International Journal of Electrical Power & Energy Systems*, 131, 107021.
- [32] Ren, C., & Xu, Y. (2022). Robustness Verification for Machine-Learning-Based Power System Dynamic Security Assessment Models Under Adversarial Examples. *IEEE Transactions on Control of Network Systems*, 9(4), 1645-1654.
- [33] Chen, Z., Ren, C., Xu, Y., Dong, Z. Y., & Li, Q. (2023). Data-driven power system dynamic security assessment under adversarial attacks: Risk warning based interpretation analysis and mitigation. *IET Energy Systems Integration*.
- [34] Liu, S., Shi, R., Huang, Y., Li, X., Li, Z., Wang, L., ... & Liu, L. (2021). A data-driven and data-based framework for online voltage stability assessment using partial mutual information and iterated random forest. *Energies*, 14(3), 715.
- [35] IEEE Standard for Synchrophasors for Power Systems, IEEE Std.C37. 118-2005.
- [36] Azad, S., Ameli, M. T., Amiri, M. M., Ameli, H., Shadi, M. R., & Strbac, G. (2024). Real-time Voltage Stability Assessment with a Novel Bus Index Considering Impact of Connection to Distribution Networks. *IEEE Access*.