International Journal of Engineering Trends and Technology
ISSN: 2231-5381/ https://doi.org/10.14445/22315381/IJETT-V74I4P101

Volume 74 Issue 4, 1-12, April 2026

Original Article

Smart Variable Selection for Static Security Assessment: A Multi-Class Support Vector Machine Framework

Astik Dhandhia[1], Jaydeepsinh Sarvaiya[2], Vivek Pandya[3]

[1,2]*Electrical Department, Shantilal Shah Engineering College, Gujarat, India.*
[3]*Electrical Department, Pandit Deendayal Energy University, Gujarat, India.*

[1]*Corresponding Author : akdhandhia@elec.ssgec.ac.in*

Received: 01 July 2025 Revised: 07 February 2026 Accepted: 12 February 2026 Published: 29 April 2026

Abstract - *To maintain a secure and stable power system, operators must make informed decisions based on the current situation. Traditional power flow techniques have several drawbacks, including their high memory requirements and lengthy computation times. As a result, they are impractical options for real-time static security assessment applications. The masking problem with the performance indexes based on changes in bus voltage and power loading of transmission lines for security assessment is addressed by formulating a composite security index; as a result, the composite security index is better able to discriminate in close-range violations. Support Vector Machines are utilised within a multiclass classification framework to address the static security issues of power systems. A new smart variable selection approach is applied for static security assessment. It is demonstrated how various power system variable sets impact the efficiency of the multiclass support vector machine classifier. For optimal feature selection, sequential forward selection is employed to maximize classification accuracy while minimizing the misclassification rate. Two standard IEEE test systems validate the results of a Multi-Class Support Vector Machine Framework with smart variable selection during training and testing.*

Keywords - *Artificial Intelligence, Power system static security assessment, Support Vector Machine, Composite security index, Feature selection.*

1. Introduction

The deregulation of big and complex power systems has resulted in an enormous rise in the demand for electric power. Operators must work relentlessly to provide a reliable and high-quality supply of electrical power to customers. Therefore, developing new, innovative, and efficient approaches to managing and controlling the power system is crucial. The power system is considered secure if it operates within safe limits during regular operation and remains stable after any disturbance [1].

Developing a fast static security assessment is one of the toughest challenges because simulation tools require a lot of calculation time and generate a lot of data. A set of algebraic equations is solved to evaluate the static security of the power grid. Power flow simulations are typically used to assess the static security; however, this process is time-intensive and not appropriate for real-time applications. Therefore, an effective solution is required for the quick evaluation of static security utilising real-time data. The Pattern Recognition (PR) approach provides a solution to the limitations of traditional power flow programs in static security assessment. The Pattern Recognition (PR) approach carries out all its main computations in offline line mode, making it feasible to find the security state of the system within a practical timeframe. The data generation process, which is utilized for training, requires these offline computations. These training data form the basis of the classifier's design, and the trained classifier provides an instantaneous assessment of static security.

Static Security Assessment (SSA) problems are addressed by artificial intelligence approaches such as the multi-layered feed-forward network [2-4], Neural Network using Radial Basis Function [5, 6], and Multilayer Perceptron [7]. The security evaluation of power systems has made use of Genetic-type Neural Networks [8], Query-based Learning type techniques [9], and random forest [10]. Static security assessment has also been explored through advanced deep learning approaches, including Convolutional Neural Networks (CNNs) [11, 12]. The previously described methods are applied to decrease the computational burden involved in real-time security assessment. The techniques discussed earlier exhibit strong problem dependency and are inadequate for anticipating future insecure operating scenarios. Among the previously used approaches, pattern-recognition-based techniques employing Support Vector Machines (SVMs) have emerged as one of the most promising solutions. Support Vector Machine (SVM)-based

techniques have been utilized for the assessment of static security in several studies [13-15]. PR is utilized for the assessment of the security index [13-15]. The weighting factor choice in the security index calculation is critical because it could lead to incorrect classifications of power system states. To prevent the masking problem, the Composite Security Index (CSI) depends on the hyper-ellipse concept embedded within a hyper-box framework. This method is described in full in [16]. To overcome the challenge of choosing an appropriate weighting factor, a Composite Security Index (CSI) framework is proposed [13-15]. The training quality and overall effectiveness of the PR approach rely heavily on the selection of power system variables used to form input patterns. Over the past four decades, a wide range of variables has been incorporated as inputs for training and evaluating PR-based models.

These include active, reactive, and apparent power flows in transmission lines; reactive and active power outputs at generator buses; reactive and active loads at various buses; bus voltage magnitudes; and bus angle. In most studies, only a subset of these variables has been used to generate the input patterns. Consequently, it is essential to examine how different variable choices influence the performance of static security assessment and to compare PR-based methods under multiple variable combinations within the same framework.

The optimized feature selection and a composite security index can accurately and efficiently assess the static security of power systems under varying operating conditions using a multiclass Support Vector Machine. The following research gaps were identified based on the prior works in the SSA of the power system:

- The performance indices used in earlier studies suffer from masking effects.
- Previously applied artificial intelligence methods demonstrate strong problem dependency and are not sufficient for predicting future insecure operating conditions.
- The influence of different power system variables on classifier performance for forecasting future secure and insecure operating states has not been adequately addressed.

Based on the above research gap, we have defined the following objectives in the security assessment for the power systems:

- To develop a composite security index that is free from masking effects and capable of classifying system patterns into secure, alarm, and insecure categories.
- To design a novel multiclass classification approach using SVM for identifying static security conditions at three levels—secure, alarm, and insecure—through PR techniques. The adoption of the Radial Basis Function (RBF) kernel, the One-Versus-One (OVO) multiclass strategy, and Sequential Forward Selection (SFS) for optimal feature selection is intended to enhance the classifier's overall performance.
- To employ an intelligent variable-selection strategy to analyze how different sets of power system variables influence the performance of a PR approach based on multiclass SVM.

The structure of the paper is as follows: Section 2 discusses the masking-free Composite Static Security Index (CSSI) for static security assessment; Section 3 presents the Pattern Recognition (PR)-based static security assessment approach; Section 4 provides the results and discussion; and Section 5 concludes the paper.

2. Composite Static Security Index for Assessment of SSA

Static security describes the capability of a power system to function within a specified range while ensuring that no constraints are violated. Moreover, following a disturbance such as the outage of a generator or a transmission line, the violations must be limited to a defined region [17-19]. Such an outage event is referred to as a contingency. When a contingency occurs, an assessment of static security is performed to identify any potential transmission line overloads or violations of bus voltage limits. The identified critical contingencies are subsequently ranked and classified by SSA according to the severity of their adverse effects on system security.

This ranking and classification process is commonly performed using a Performance Index (PI) derived from load flow solutions. However, the masking phenomenon significantly influences the accuracy of contingency ranking and classification [19, 20]. To address the masking problem with the traditional performance indices, an improved method for computing the CSI was presented in [16], based on a hyper-ellipse embedded within a hyper-box.

2.1. Development of Composite Static Security Index

The conditions defined in (1)–(2) must be satisfied during normal operating conditions of the power system.

$$\sum_{a=1}^{N_{Gen}} P_{G-a} = P_{T-L} + P_{T-loss} \tag{1}$$

$$\left.\begin{array}{c} P_{G-a}^{min} \le P_{G-a} \le P_{G-a}^{max}, a = 1, 2, \dots, N_{Gen} \\ \left|\left|V_{B-a}^{min}\right| \le |V_{B-a}| \le |V_{B-a}^{max}|\right|, a = 1, 2, \dots, N_{Bus} \\ P_{xy} \le P_{xy}^{max} \; for \; every \; branch, \; x - y \end{array}\right\} \tag{2}$$

The degree of satisfaction with constraints in (1) and (2) following an outage may indicate the "secure state" of the system. Conversely, the power system state is classified as an

"insecure state" if any of the constraints in (1) and (2) are violated. The constraints set in (2) for transmission line power flows and voltages at the bus are further sorted for security and alarm limits in the formulation of CSSI.

In this study, only upper-limit violations are considered for transmission line loading; for bus voltage violations, both upper and lower-limit violations are taken into account when determining the alarm, secure, and insecure states of bus voltages.

The state of the power system is defined as either insecure, secure, or alarm according to the criteria listed in the upcoming section, depending on the value of the CSSI.

2.1.1. Bus Voltage Static Security Index

Set V^d_{B-a}, A^u_{B-a}, A^l_{B-a}, $S^u_{B-a}$and S^l_{B-a} at bus a and calculate $a^u_{(V,a)}$, $b^u_{(V,a)}$, $a^l_{(V,a)}$and $b^l_{(V,a)}$.

$$\left.\begin{array}{l} a^u_{(B,a)} = [V_{B-a} - A^u_{B-a}]/(V^d_{B-a}); if\ V_{B-a} > A^u_{B-a} \\ a^l_{(B,a)} = [A^l_{B-a} - V_{B-a}]/(V^d_{B-a}); if\ V_{B-a} < A^l_{B-a}; \\ a^u_{(B,a)} = 0; \qquad if\ A^l_{B-a} \le V_{B-a} \le A^u_{B-a} \\ and\ a = 1,2,\dots,N_{Bus} \end{array}\right\} \quad (3)$$

$$\left.\begin{array}{l} b^u_{(B,a)} = [S^u_{B-a} - A^u_{B-a}]/(V^d_{B-a}) \\ b^l_{(B,a)} = [A^l_{B-a} - S^l_{B-a}]/(V^d_{B-a}) \\ and\ a = 1,2,\dots,N_{Bus} \end{array}\right\} \quad (4)$$

After setting $k = 1.0$, in equations (3) and (4) of the hyper-ellipse formulation [16], we can calculate the bus voltage security index as (5).

$$PI_V = \left[\sum_a \left(a^u_{(B,a)}/b^u_{(B,a)}\right)^{2k} + \sum_a \left(a^l_{(B,a)}/b^l_{(B,a)}\right)^{2k}\right]^{1/2k} \quad (5)$$

Using (5), the power system state associated with bus voltage static security can be easily identified and subsequently classified as shown in (6).

$$\left.\begin{array}{l} PI_V = 0; Secure \\ 0 < PI_V < 1; Alarm \\ PI_V \ge 1; Insecure \end{array}\right\} \quad (6)$$

2.1.2. Transmission Line Power Flow Static Security Index

The transmission line power flow static security index is computed by considering only the upper limits, as the primary concern lies in preventing excessive transmission line power flow. Calculate $c_{P,x}$ and $d_{P,x}$ for thex^{th}line.

The operating state of the power system is evaluated using the line power flow static security index, which is formulated in equations (7) and (8). The index value is obtained from (9), and the corresponding system state is subsequently classified as defined in (10).

$$c_{P,x} = \left[|P_x| - A_{P,x}\right]/Base\ MVA\ if\ |P_x| > A_{P,x}$$

$$c_{P,x} = 0 \quad if\ \left|P_x < A_{p,x}\right|, and\ x = 1,2,..,N_{line} \quad (7)$$

$$d_{P,x} = \left[S_{P,x} - A_{P,x}\right]/Base\ MVA,\ x = 1,2,..,N_{line} \quad (8)$$

$$PI_P = \left[\sum_b \left(c_{P,x}/d_{P,x}\right)\right]^{1/2k} \quad (9)$$

$$\left.\begin{array}{l} PI_P = 0; Secure \\ 0 < PI_P < 1; Alarm \\ PI_P \ge 1; Insecure \end{array}\right\} \quad (10)$$

Using the hyper-ellipse approach enclosed within the hyper-box, equations 5 and 9 can be put together to form a CSSI, as expressed in (11).

The masking issue will be effectively addressed by CSSI, enabling contingency violations to be ranked in descending order according to their CSSI values. As mentioned in (12), the CSSI value serves as a basis for evaluating the overall security status.

$$PI_C = \left[\sum_a \left(a^u_{(B,a)}/b^u_{(B,a)}\right)^{2k} + \sum_a \left(a^l_{(B,a)}/b^l_{(B,a)}\right)^{2k} + \sum_b \left(c_{P,x}/d_{P,x}\right)^{2k}\right]^{1/2k} \quad (11)$$

$$\left.\begin{array}{l} PI_C = 0; Secure \\ 0 < PI_C < 1; Alarm \\ PI_C \ge 1; Insecure \end{array}\right\} \quad (12)$$

3. Pattern Recognition (PR) based Static Security Assessment

Static security assessment is categorized into three classes: secure, insecure, and alarm. The system operator will make an informed and accurate decision regarding the static security of the system based on the predicted classification.

The implementation of the PR approach in this study has effectively reduced the calculation effort of online calculations by doing many simulation tasks offline.

Offline simulations are conducted to generate a broad range of operating scenarios, which are subsequently used as the basis for developing static security classifiers. This classifier will be directly applied in online applications to enhance the speed of assessment of static security. Figures 1 and 2 provide details of the steps followed during the generation of data sets, design of a multi-classifier, and its implementation to evaluate power system static security.

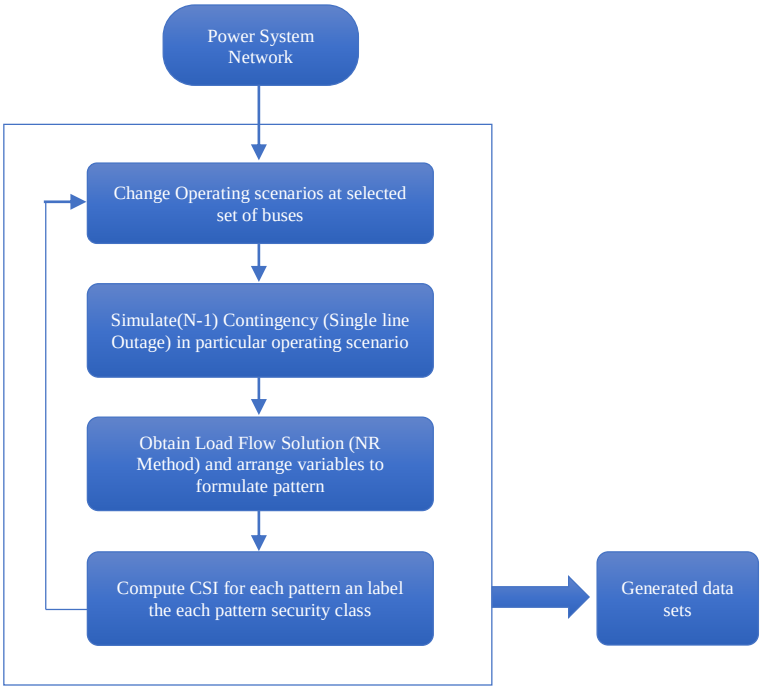

Fig. 1 Steps followed during data sets generation

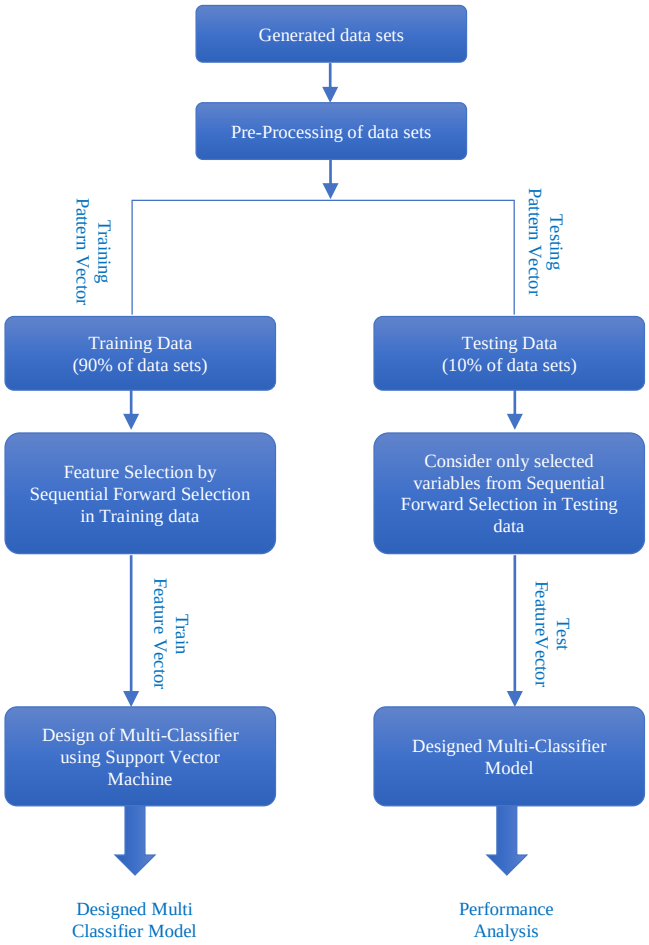

Fig. 2 Steps involved in designing and implementing a multi-class approach for assessment of static security

3.1. Generation of Pattern for Security Assessment and Smart Variable Selection for Static Security Assessment

Creating an adequate training dataset is essential for the effectiveness of any Pattern Recognition (PR) technique. This dataset should cover a diverse range of operating conditions of the power system, including variations in reactive and active power demands at the buses where loads are connected. It should also account for contingency scenarios involving generators and transmission lines that may impact overall system security. The offline data generated is considered a "pattern" [21]. The active and reactive power demands at the selected load buses are varied between 50% and 150% of their base-case values. In addition, the active power generation at generator buses is appropriately adjusted to satisfy the conditions specified in (1).

Furthermore, contingencies such as generator outages or transmission line failures, along with load fluctuations, have a significant impact on the static security of the power system. Here, a sequential process of individual transmission line failures is implemented. A total of 975 and 9,790 datasets were generated for the IEEE 30-bus and 118-bus test systems, respectively, using offline simulations in MATPOWER, encompassing a wide range of operating scenarios. For the last four decades, researchers have utilized many variables to establish the patterns, which are presented in Table 1. It is critical to select variables that accurately describe the overall behavior and condition of the system. Consequently, in the present study, it is crucial to analyze the impact of different combinations of variables on system performance.

Table 1. Different sets of variables are used in the literature for pattern recognition

	Set of selected variables
Pang et al. 1974 [21]	$\lvert V_{B-a}\rvert, \delta_{B-a}, P_{G-a}, Q_{G-a}, P_{Da}, Q_{Da}, P_{loss}, Q_{loss}, P_{G-a}^{max} - P_{G-a}, Q_{G-a}^{max} - Q_{G-a}, Q_{G-a} - Q_{G-a}^{min}, P_{T-G}, Q_{T-G}, P_{T-L}, Q_{T-L}, \sum(P_{G-a}^{max} - P_{G-a}), \sum(P_{G-a} - P_{G-a}^{min}), \sum(Q_{G-a}^{max} - Q_{G-a}), \sum(Q_{G-a} - Q_{G-a}^{min})$
Sidhu & Cui 2000 [3]	$P_{G-a}, Q_{G-a}, P_{Da}, Q_{Da}, k_i$
Jain et al. 2003 [5]	P_{Da}, Q_{Da}
Mohammadi & Gharehpetian 2009 [22]	$\lvert V_{B-a}\rvert, P_{G-a}, Q_{G-a}, P_{Da}, Q_{Da}, P_{xy}, Q_{xy}, S_{xy}$
Kalyani & Swarup [14, 15, 23]	$\lvert V_{B-a}\rvert, \delta_{B-a}, S_{G-a}, S_{Da}, S_{xy}$
Sunitha et al. 2013 [24]	$\lvert V_{B-a}\rvert, \delta_{B-a}, P_{G-a}, Q_{G-a}, P_{Da}, Q_{Da}$
Sekhar & Mohanty 2016 [25]	$\lvert V_{B-a}\rvert, P_{G-a}, Q_{G-a}, P_{Da}, Q_{Da}, k_i$

This study explores how the selection of different variable sets influences the effectiveness of the classification model. The total number of sets considered is five, as shown in (13-17).

Therefore, load flow is performed for each operating state, resulting in the formation of a pattern with the parameters listed in (13-17). The decision chosen by CSI (11) will classify the power system into one of three states: secure, alarm, or insecure.

$$X_1 = \{|V_{B-a}|, \delta_{B-a}\} \quad (13)$$

$$X_2 = \begin{Bmatrix} |V_{B-a}|, \delta_{B-a}, Contingency\ number\ in \\ binary\ form \end{Bmatrix} \quad (14)$$

$$X_3 = \{|V_{B-a}|, \delta_{B-a}, P_{Gen-a}, Q_{Gen-a}, P_{Da}, Q_{Da}\} \quad (15)$$

$$X_4 = \begin{Bmatrix} |V_{B-a}|, \delta_{B-a}, P_{Gen-a}, Q_{Gen-a}, \\ P_{Da}, Q_{Da}, Contingency \\ no.\ in\ binary\ form \end{Bmatrix} \quad (16)$$

$$X_5 = \{|V_{B-a}|, \delta_{B-a}, P_{G-a}, Q_{G-a}, P_{Da}, Q_{Da}, P_{xy}, Q_{xy}\} \quad (17)$$

3.2. Feature Selection

Each pattern comprises a large number of variables, and as indicated in (13–17), the dimensionality of the pattern tends to increase with the size of the power system. Feature selection, which involves extracting a reduced subset of variables (referred to as features) from the original variable set defined in (13)–(17), is therefore employed to decrease the dimensionality of the feature vector.

The selected subset forms a feature vector $Z = \{z_1, z_2, .., z_m\}$, where m is significantly smaller than the total variables in the original feature vector. However, during the process of selecting a limited set of features from a large variable set, the exclusion of certain critical variables can negatively affect the classifier's accuracy and result in an increased misclassification rate. In this study, the feature selection process employs Sequential Forward Selection (SFS), where variables are added one by one to the feature vector in a step-by-step process. It operates by minimizing the objective function, as given in equation (18). Starting with an empty set of features, the SFS method sequentially adds each feature until it becomes impossible to maximize the objective function further.

3.3. Design of Multi-Class Support Vector Machine Framework

The SFS method is highly advantageous for extracting an optimum feature vector. The feature vector will be used as the input pattern for classifier design. The various distinctions between secure, alarm, and insecure classes are established by the classifier. Training patterns are necessary for the classifier's development, and they are validated by unidentified testing patterns. The classifier is designed using a variety of methods, such as the KNN (k-nearest-neighbor) approach, the least-squares approach, and back-propagation type neural net classifiers [21]. The adoption of more reliable and accurate training techniques, including Support Vector Machine (SVM), was prompted by the inadequacies of the existing multi-class classifier design. SVMs are newly identified machine learning approaches used for solving classification problems. They have demonstrated high accuracy, even in complicated systems.

Let $A = \{m_i, n_i\}$ be the training set, where, m_i is an input vector has a specified n −dimension. $n_i \in \{+1, -1\}$ acts as the label during determining the class of a data instance n_i.

The optimum hyperplane of the SVM classifier is seen in Figure 3 for a two-class problem, where the bias $b$and weight $w$are two perpendicular vectors. Figure 3 shows Support vectors (SVs) and is identified as those points that are closest to the hyperplane that develops. The margin shown in Figure 3 is the maximum margin to be allocated for forming SVs. SVM creates the optimal hyperplane by reducing the error function through iterative training.

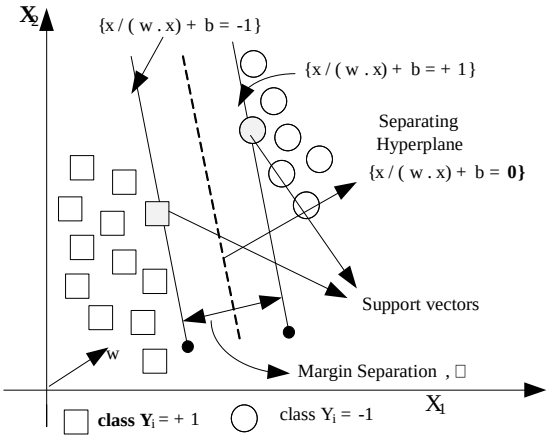

Fig. 3 The representation of optimal hyper plane for binary classifier of SVM

This work considers three classes for power system security: secure, alarm, and insecure. This work treats this type of pattern classification problem as a multiclass problem, because a single SVM formulation cannot solve it. The present research developed an approach to address this drawback by integrating multiple SVM binary classifiers. The One-Versus-One (OVO) and One-Versus-All (OVA) are two widely used strategies for handling multiclass classification problems with Support Vector Machines (SVMs). Compared to the OVA method, the OVO approach typically demands significantly less training data for model training [26]. Let K classes be classified for the problem. The OVO-SVM technique is used to formulate binary classifiers$k(k-1)\,/\,2$. Each binary classifier's training data is only known based on its respective classes. For $p^{th}$and q^{th}class, from training data, Equation (18) is resolved as an optimization problem. Where b is the threshold and $\Phi(*)$ is the Kernel mapping function. In this instance, classification is done using the "Max-Wins voting" method [25].

$$\left.\begin{array}{l} Min\ {}_{w^{pq},b^{pq},\zeta^{pq}}\ \frac{1}{2}(w^{pq})^T w^{pq} + c\sum_{j=1}^{N}\zeta_t^{pq} \\ subjected\ to \\ (w^{pq})^T\Phi(x_t) + b^{pq} \geq 1 - \zeta_t^{pq}, for\ y_t = p \\ (w^{pq})^T\Phi(x_t) + b^{pq} \geq -1 + \zeta_t^{pq}, for\ y_t = q \\ \zeta_t^{pq} \geq 0 \end{array}\right\} \quad (18)$$

3.3.1. SVM Parameters Selection Approach

The Radial Basis Function (RBF) kernel is widely favored for SVMs due to its ability to model nonlinear relationships between class labels and selected features, while also offering high Classification Accuracy (CA) and a low Misclassification Rate (MCR) [27]. The optimum values of the hyperparameters (c, γ) are determined using v-fold cross-validation in conjunction with a grid search strategy. The highest level of accuracy in cross-validation can be achieved by choosing the best possible optimum values of the hyperparameters (c, γ). The combinations of $\{2^{-5}, 2^{-4}, \ldots, 2^{14}, 2^{15}\}$ and $\{2^{-15}, 2^{-14}, \ldots, 2^{4}, 2^{5}\}$ are chosen for c and γ, respectively. Grid search and five-fold cross-validation together ensure better management of bias and variance during model training and testing. Correctly determining the state of the power system in any PR approach requires the classifier's Classification Accuracy (CA) to be as high as possible and the Misclassification Rate (MCR) to be as minimal as possible, as shown in (19) and (20), respectively.

3.3.2. Performance Evaluation Terms

$$CA\ (\%) = \frac{Total\ correctly\ classified\ patterns}{Total\ patterns\ in\ data\ set} \times 10 \quad (19)$$

$$\text{MCR}(\%) = \frac{\text{No. of misclassifications occurs in k}^{\text{th}}\text{ class}}{\text{Total no. of patterns in k}^{\text{th}}\text{class}} \times 100 \quad (20)$$

4. Results and Discussions

A multiclass support vector machine framework by using optimized features implemented on the small IEEE 30 bus (Power network-I), and large IEEE 118-bus (Power network-II) systems to validate the findings obtained with multi-class SVM. These test systems cover a range of system sizes, including both small and large systems. The active and

reactive power demands on individual buses have been changed to vary from 50% to 150% of their baseline levels. In addition, a one-line contingency analysis has been conducted for each load variation situation to produce a larger set of appropriate patterns for assessment of static security. The active power output of generator buses at PV buses is adjusted in response to variations in load demand while also considering the maximum and minimum capacity for the generation of reactive power.

There might be masking issues with security assessments that focus just on the constraints outlined in (1) and (2) [16, 20]. Therefore, in this article, the CSSI talk through in Section 2 and defined by Equation (11) has been employed to evaluate static security in order to address this problem. CSI can accurately and efficiently assess the static security of power systems under varying operating conditions using a multiclass Support Vector Machine. Multi-class Support Vector Machines (SVM) classify the security statuses into secure, insecure, and alarm classes. The alarm and security limits for voltage deviations from the nominal value of 1 per unit (pu) are set at ± 5% and ± 7%, respectively, for all load buses. In order to maintain the specified magnitude of the bus voltage for the generator bus, it is essential for the reactive power to remain within its defined lower and upper limits. For the test systems considered in this study, the alarm threshold for loading in the transmission line is set at 80% of the defined security limits. Table 2 shows that a total of 975 and 9,790 operating patterns were generated for the Power network-I and II, respectively, using simulations conducted with the MATPOWER toolbox.

Table 2. Classification of generated patterns into secure case, alarm case, and insecure case

	Power network-I	**Power network -II**
Overall operating cases	975 (819+156)	9790 (8722+1068)
Secure cases (Training cases + Testing cases)	382 (297+87)	6708 (5938 +770)
Alarm Cases (Training Cases + Testing Cases)	361 (317+42)	2371 (2153+218)
Insecure Cases (Training Cases + Testing Cases)	232 (205+27)	711 (631+80)

These patterns encompass a wide range of operating conditions. Based on the Composite Static Security Index (CSSI), the generated patterns were classified into secure, alarm, and insecure cases, as summarized in Table 2. The complete dataset of patterns was divided such that 90% were used for training, while the remaining 10% were reserved for testing. The selection of appropriate features enhances classification accuracy while reducing the misclassification rate. The present research utilizes the sequential forward selection technique, as it produces the most effective results for feature selection [14].

Table 3 illustrates how the SFS approach reduces the size of the power networks under study. The feature dimensionality was reduced using the Sequential Forward Selection (SFS) method by up to 8.88% and 7.14% for the Power network -I and II, respectively, as shown in Table 3. Figures 4–13 show Cross Validation (CV) charts for optimal (c, γ) solutions for the two power networks I and II under consideration. Figures 4–13 indicate optimum values (c, γ) and cross-validation accuracy levels for small power network-I, and large power network-II using Grid search (GS) with 5-fold cross-validation. The optimal parameter values were chosen based on the highest cross-validation accuracy achieved. The selected optimal parameters along with their corresponding cross-validation accuracies are illustrated in Figures 4–13.

A Multi-Class Support Vector Machine Framework's testing reveals that the selected pattern, as shown in (14) for both power networks, yields a higher classification. The five multi-class support vector frameworks were trained using the patterns defined in Equations (13)–(17) with the same training dataset. Subsequently, all five trained frameworks were evaluated using the same testing dataset.

The unseen data were used as testing datasets to evaluate the trained framework, ensuring an unbiased assessment of its performance. The results showed that for both power networks, the selected pattern given in (14) achieved the highest accuracy during testing. The results also revealed that seven and ten misclassifications occur in the small test power network-I and large power network-II, respectively. It is also seen that two and one insecure misclassifications occur in the power network-I and power network-II, respectively.

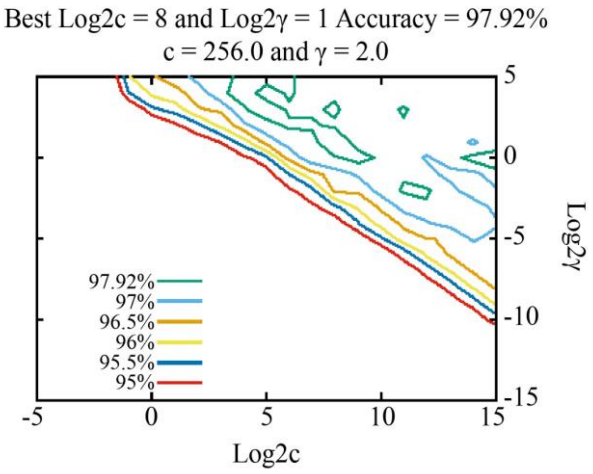

Fig. 4 Five-fold cross-validation curve derived from grid search for Equation (13) in the power network-I

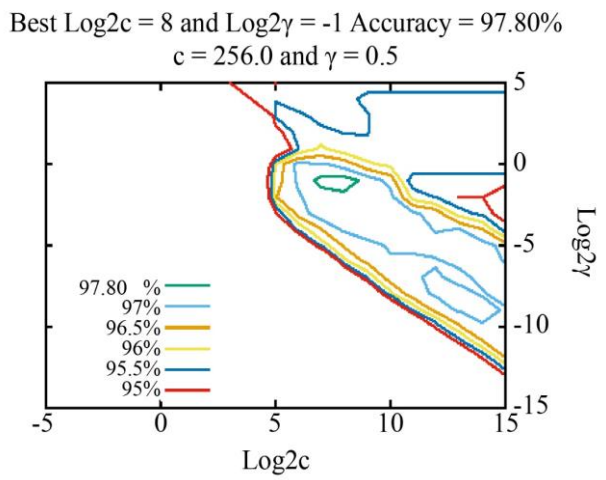

Fig. 5 Five-fold cross-validation curve derived from grid search for Equation (14) in the power network -I

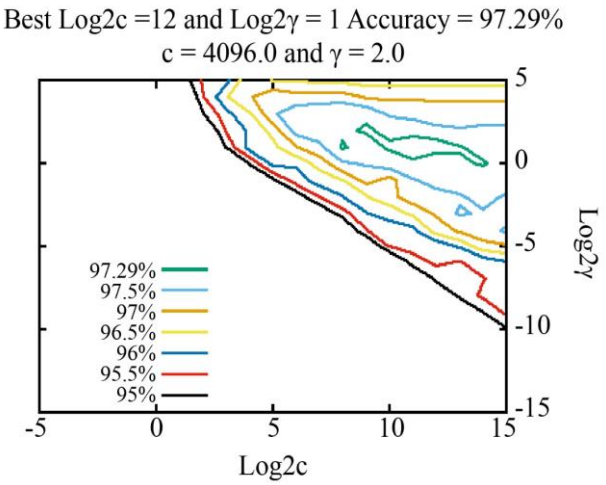

Fig. 6 Five-fold cross-validation curve derived from grid search for Equation (15) in the power network -I

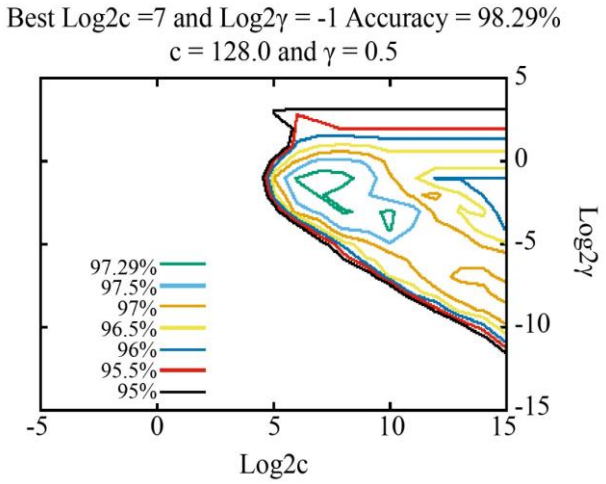

Fig. 7 Five-fold cross-validation curve derived from grid search for Equation (16) in the power network-I

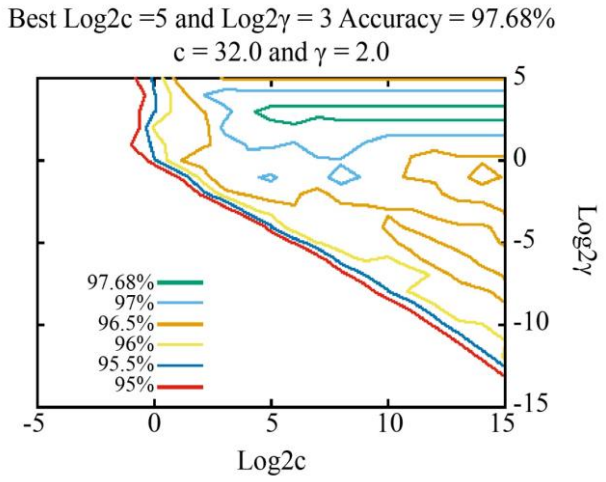

Fig. 8 Five-fold cross-validation curve derived from grid search for Equation (17) in the power network-I

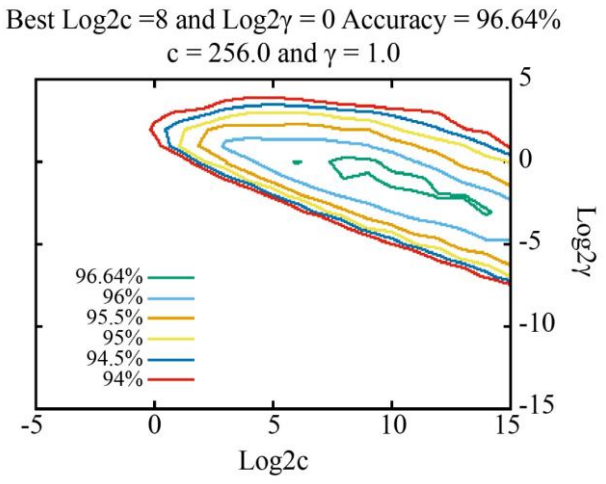

Fig. 9 Five-fold cross-validation curve derived from grid search for Equation (13) in the power network-II

Fig. 10 Five-fold cross-validation curve derived from grid search for Equation (14) in the power network-II

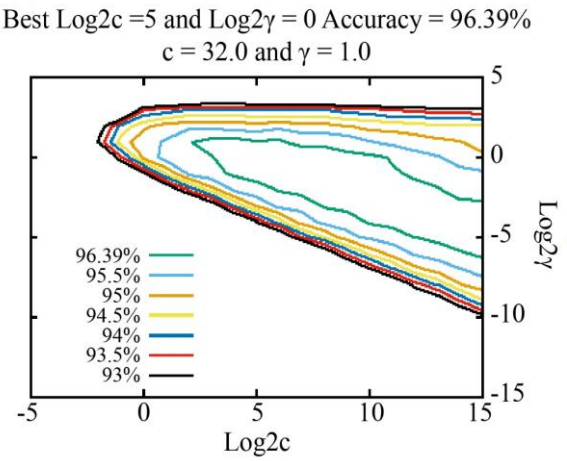

Fig. 11 Five-fold cross-validation curve derived from grid search for Equation (15) in the power network-II

The results showed that for both power networks, the selected pattern given in (14) achieved the highest accuracy during testing. The results also revealed that seven and ten misclassifications occur in the small power network-I and large power network-II, respectively. It is also seen that two and one insecure misclassifications occur in the power network-I and power network-II, respectively. For power network-I, the highest testing accuracy of 98.25% was achieved using the variables specified in Eq. (14).

It is also noticed that the larger-sized power network has reached 99.06% percent testing accuracy in the selected pattern given X_2 in (14). In such cases, the proposed multi-class support vector machine framework performs exceptionally well when the selected pattern set is X_2 as given in (14). We discover that bus voltages, voltage angles, and the contingency number represented in binary form provide adequate information to classify the state of the power system during the assessment of static security.

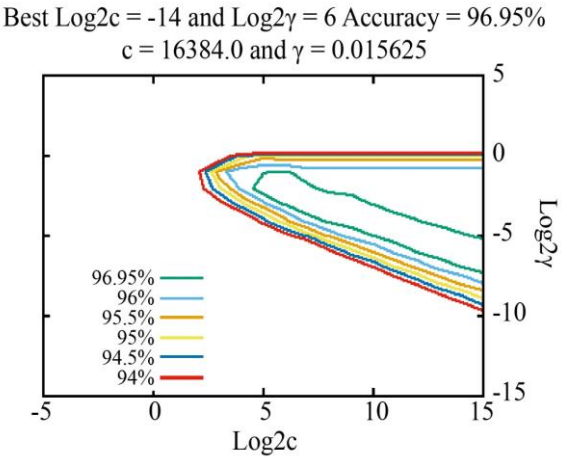

Fig. 12 Five-fold cross-validation curve derived from grid search for Equation (16) in the power network-II

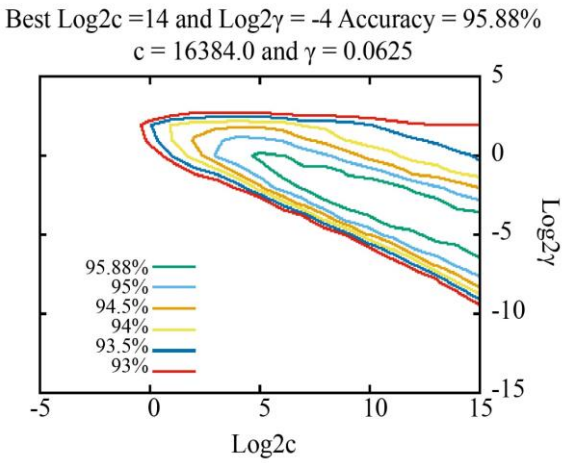

Fig. 13 Five-fold cross-validation curve derived from grid search for Equation (17) in the power network-II

Table 1. Dimensionality reduction following feature selection

	Power Network-I	**Power Network-II**
Total pattern variable in $\boldsymbol{X_1}$ as in equation (13)	53	180
Total pattern variable $\boldsymbol{X_2}$ as in equation (14)	59	188
Total pattern variable $\boldsymbol{X_3}$ as in equation (15)	102	424
Total pattern variable $\boldsymbol{X_4}$ as in equation (16)	108	432
Total pattern variable $\boldsymbol{X_5}$ as in equation (17)	214	952
Selected features from the pattern $\boldsymbol{X_1}$, $\boldsymbol{X_3}$, and $\boldsymbol{X_5}$	13	60
Selected features from the pattern $\boldsymbol{X_2}$ and $\boldsymbol{X_4}$	19	68
% Reduction in dimension in pattern $\boldsymbol{X_1}$, $\boldsymbol{X_3}$, and $\boldsymbol{X_5}$	6.08%	6.30%
% Reduction in dimension in pattern $\boldsymbol{X_2}$ and $\boldsymbol{X_4}$	8.88%	7.14%

The superior performance of the proposed approach results from several key factors, including an optimized feature selection strategy and effective hyperparameter tuning using grid search with five-fold cross-validation. Missing data were carefully managed, and a well-structured preprocessing pipeline was applied to enhance data quality, leading to improved prediction accuracy. Moreover, the efficient model architecture enables faster learning and more precise predictions compared to state-of-the-art methods reported in the literature [14, 15, 23]. The model generates predictions within 1-2 seconds, making it suitable for real-time online applications. Additionally, a masking-problem-free composite security index allows accurate and efficient assessment of the static security of power systems under varying operating conditions using a multiclass Support Vector Machine.

Table 4. Performance of analysis of multi-class SVM classifier for power network-I

	Training sets	Testing Set				
Selected Pattern Vector	**CA (%)**	**CA (%)**	**MCR (%) (Secure)**	**MCR (%) (Alarm)**	**MCR (%) (Insecure)**	**Overall CA (%) (Training & Testing)**
X_1as in equation (13)	98.53% (807/819)	93.59% (146/156)	5.75% (5/87)	7.14% (3/42)	7.41% (2/27)	97.74% (953/975)
X_2 as in equation (14)	98.78% (809/819)	95.51% (149/156)	3.45% (3/87)	4.76% (2/42)	7.41% (2/27)	98.25% (958/975)
X_3 as in equation (15)	99.76% (817/819)	94.23% (147/156)	5.75% (5/87)	2.38% (1/42)	11.11% (3/27)	98.87% (964/975)
X_4 as in equation (16)	99.27% (813/819)	92.95% (145/156)	10.34% (9/87)	4.76% (2/42)	0% (0/27)	98.25% (958/975)
X_5 as in equation (17)	100% (819/819)	94.23% (147/156)	3.45% (3/87)	9.52% (4/42)	7.41% (2/27)	99.08% (966/975)

Table 5. Performance of analysis of a multi-class SVM classifier for power network-II

	Training sets	Testing Sets				
Selected Pattern Vector	**CA (%)**	**CA (%)**	**MCR (%) (Secure)**	**MCR (%) (Alarm)**	**MCR (%) (Insecure)**	**Overall CA (%) (Training & Testing)**
X_1as in equation (13)	98.74% (8612/8722)	98.97% (1057/1068)	0.52% (4/774)	1.87% (4/214)	3.75% (3/80)	98.76% (9669/9790)
X_2 as in equation (14)	99.35% (8665/8722)	99.06% (1058/1068)	0.78% (6/774)	1.40% (3/214)	1.25% (1/80)	99.32% (9723/9790)
X_3 as in equation (15)	98.18% (8563/8722)	99.06% (1058/1068)	0.39% (3/774)	1.87% (4/214)	3.75% (3/80)	98.27% (9621/9790)
X_4 as in equation (16)	98.73% (8611/8722)	98.03% (1047/1068)	1.29% (10/774)	4.67% (10/214)	1.25% (1/80)	98.65% (9658/9790)
X_5 as in equation (17)	98.34% (8577/8722)	97.47% (1041/1068)	2.71% (21/774)	1.87% (4/214)	2.50% (2/80)	98.24% (9618/9790)

5. Conclusion

This research paper proposes an optimized feature selection approach and a masking problem-free composite static security index to assess the security of a power system using pattern recognition-based multi-class Support Vector Machine. The composite static security index avoids the masking problem by precisely discriminating between alarm, secure, and insecure cases, even near constraint violations. The alarm limitations enable the operator to comprehend the power system's static security early on and make any required corrections beforehand. Support Vector Machines (SVMs) are effectively employed to develop a multiclass classifier that categorizes system operating states into secure, alarm, and insecure conditions. In this manner, the pattern recognition problem becomes a multi-class problem. The Sequential Forward Selection approach reduces pattern dimensionality through effective feature extraction, thereby enhancing classification accuracy and reducing misclassification rates. The optimized feature selection approach demonstrates how different sets of power system variables influence the performance of a multi-class SVM classifier. The five multi-class support vector frameworks were formulated using the patterns defined in Equations (13)-(17). All five multi-class classifier models achieved overall accuracies exceeding 97% across both power network I and II, demonstrating the effectiveness and robustness of the proposed approach. Notably, the accuracy was even higher for the larger and more complex power network-II. For the power networks I and II, the highest testing accuracies of 98.25% and 99.06%, respectively, were achieved using the variables specified in Equation (14). This indicates that bus voltages, voltage angles, and binary-encoded contingency numbers effectively capture the critical characteristics of the power system state.

References

[1] Kip Morison, Lei Wang, and Prabha Kundur, "Power System Security Assessment," *IEEE Power Energy Magazine*, vol. 2, no. 5, pp. 30-39, 2004. [CrossRef] [Google Scholar] [Publisher Link]

[2] Tarlochan S. Sidhu, and Lan Cui, "Contingency Screening for Steady-State Security Analysis by using FFT and Artificial Neural Networks," *IEEE Transactions on Power Systems*, vol. 15, no. 1, pp. 421-426, 2000. [CrossRef] [Google Scholar] [Publisher Link]

[3] Khaleequr Rehman Niazi, Chandra Mohan, and Simrath L. Surana, "Power System Security Evaluation using ANN: Feature Selection using Divergence," *Electric Power Systems Research*, vol. 69, no. 2-3, pp. 161-167, 2004. [CrossRef] [Google Scholar] [Publisher Link]

[4] N. Aishwarya, and Shekhappa G. Ankaliki, "AI based Static Security Assessment of Power System," *I-Manager's Journal on Power Systems Engineering*, vol. 8, no. 2, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] Trapti Jain, L. Srivastava, and Sri Niwas Singh, "Fast Voltage Contingency Screening using Radial Basis Function Neural Network," *IEEE Transactions on Power Systems*, vol. 18, no. 4, pp. 1359-1366, 2003. [CrossRef] [Google Scholar] [Publisher Link]

[6] Rakesh Kumar Misra, and Shiv Pujan Singh, "Efficient ANN Method for Post-Contingency Status Evaluation," *International Journal of Electrical Power and Energy Systems*, vol. 32, no. 1, pp. 54-62, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[7] David L. Alvarez et al., "*N - K* Static Security Assessment for Power Transmission System Planning using Machine Learning," *Energies*, vol. 17, no. 2, pp. 1-17, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] Azah Mohamed, Sheikh Maniruzzaman, and Aini Hussain, "Static Security Assessment of a Power System using Genetic-based Neural Network," *Electric Power Components and Systems*, vol. 29, no. 12, pp. 1111-1121, 2001. [CrossRef] [Google Scholar] [Publisher Link]

[9] S.-J. Huang, "Static Security Assessment of a Power System using Query-based Learning Approaches with Genetic Enhancement," *IEEE Proceedings-Generation, Transmission and Distribution*, vol. 148, no. 4, pp. 319-325, 2001. [CrossRef] [Google Scholar] [Publisher Link]

[10] Nanang Hariyanto et al., "Study of Static Security Assessment Accuracy Results using Random Forest with Various Types of Training and Test Datasets," *International Journal on Electrical Engineering and Informatics*, vol. 15, no. 1, pp. 119-133, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] M. Ramirez-Gonzalez, Felix Rafael Segundo-Sevilla, and Peter Korba, "Convolutional Neural Network based Approach for Static Security Assessment of Power Systems," *2021 World Automation Congress (WAC)*, Taipei, Taiwan, pp. 106-110, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] Miguel Ramirez-Gonzalez et al., "Convolutional Neural Nets with Hyperparameter Optimization and Feature Importance for Power System Static Security Assessment," *Electric Power Systems Research*, vol. 211, pp. 1-8, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] M. Mohammadi, and G.B. Gharehpetian, "Power System On-Line Static Security Assessment by using Multi-Class Support Vector Machines," *Journal of Applied Sciences*, vol. 8, no. 12, pp. 2226-2233, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[14] S. Kalyani, and Shanti K. Swarup, "Classifier Design for Static Security Assessment using Particle Swarm Optimization," *Applied Soft Computing*, vol. 11, no. 1, pp. 658-666, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[15] S. Tara Kalyani, and K. Shanti Swarup, "Classification and Assessment of Power System Security using Multiclass SVM," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 41, no. 5, pp. 753-758, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[16] R. Sunitha, R. Kumar Sreerama, and Abraham T. Mathew, "A Composite Security Index for On-Line Steady-State Security Evaluation," *Electric Power Components and Systems*, vol. 39, no. 1, pp. 1-14, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[17] Mohammad Shahidehpour, and Yaoyu Wang, *Communication and Control in Electric Power Systems: Applications of Parallel and Distributed Processing*, John Wiley and Sons, 2003. [Google Scholar] [Publisher Link]

[18] G.C. Ejebe, H. Van Meeteren, and Bruce Wollenberg, "Fast Contingency Screening and Evaluation for Voltage Security Analysis," *IEEE Transaction on Power Systems*, vol. 3, no. 4, pp. 1582-1590, 1988. [CrossRef] [Google Scholar] [Publisher Link]

[19] Allen J. Wood, Bruce F. Wollenberg, and Gerald B. Sheblé, *Power Generation, Operation, and Control*, 3rd ed., John Wiley and Sons, 2013. [Google Scholar] [Publisher Link]

[20] K. Nara et al., "On-Line Contingency Selection for Voltage Security Analysis," *IEEE Transaction on Power Apparatus System*, vol. PAS-104, no. 4, pp. 846-856, 1985. [CrossRef] [Google Scholar] [Publisher Link]

[21] C.K. Pang et al., "Security Evaluation in Power Systems using Pattern Recognition," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-93, no. 3, pp. 969-976, 1974. [CrossRef] [Google Scholar] [Publisher Link]

[22] M. Mohammadi, and G. Gharehpetian, "Application of Core Vector Machines for On-Line Voltage Security Assessment using a Decision-Tree-based Feature Selection Algorithm," *IET Generation, Transmission and Distribution*, vol. 3, no. 8, pp. 701-712, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[23] S. Kalyani, and K. Shanti Swarup, "Design of Pattern Recognition System for Static Security Assessment and Classification," *Pattern Analysis and Applications*, vol. 15, no. 3, pp. 299-311, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[24] R. Sunitha, R. Sreerama Kumar, and Abraham T. Mathew, "Online Static Security Assessment Module using Artificial Neural Network," *IEEE Transactions on Power Systems*, vol. 28, no. 4, pp. 4328-4335, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[25] Pudi Sekhar, and Sanjeeb Mohanty, "An Online Power System Static Security Assessment Module using Multi-Layer Perceptron and Radial Basis Function Network," *International Journal of Electrical Power and Energy Systems*, vol. 76, pp. 165-173, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[26] Chih-Wei Hsu, and Chih-Jen Lin, "A Comparison of Methods for Multiclass Support Vector Machines," *IEEE Transaction on Neural Networks*, vol. 13, no. 2, pp. 415-425, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[27] Jae H. Min, and Young-Chan Lee, "Bankruptcy Prediction using Support Vector Machine with Optimal Choice of Kernel Function Parameters," *Expert Systems with Applications*, vol. 28, no. 4, pp. 603-614, 2005. [CrossRef] [Google Scholar] [Publisher Link]

List of Nomenclature

P_{G-a}, Q_{G-a}	Active and reactive power generation at the generator at bus a, respectively.	S^{u}_{B-a}, S^{l}_{B-a}	Upper and lower security bus voltage limit at bus a, respectively.
P_{T-loss}	Total transmission line active loss	N_{Gen}	Number of generators
ζ_t^{pq}	Slack variable of pair $p-q$	w^{pq}	Hyperplane weight vector of pair $j-k$
P_{xy}, Q_{xy}	Active and reactive power flow in the transmission line $x-y$, respectively.	$\|P_x\|$	Active power flow in the transmission line x
P^{min}_{G-a}	Minimum generation of active power at bus a	$A_{P,x}$	Active power alarm limit in transmission line x
k_i	Contingency outage number	$S_{P,x}$	Thermal limit in transmission line x
N_{Bus}	Number of buses	δ_{B-a}	Bus angle at bus a
$\|V^{min}_{B-a}\|$	Minimum limit of bus voltage at bus a	$\|V^{max}_{B-a}\|$	Maximum limit of bus voltage at bus a
P^{max}_{G-a}	Maximum generation of active power at bus a	Q_{Da}, P_{Da}	Reactive and active load power at bus a, respectively.
V^{D}_{B-a}	Desired bus voltage at bus a	$\|V_{B-a}\|$	Voltage magnitude at bus a
P^{max}_{xy}	Maximum limit of active power flow in transmission line $x-y$	P_{loss}, Q_{loss}	Total active and reactive power losses of the transmission line, respectively.
Q_{T-G}, P_{T-G}	Total generated reactive and active power, respectively.	$Q^{min}_{G-a}, Q^{max}_{G-a}$	Minimum and maximum generation of reactive power at bus a, respectively.
A^{u}_{B-a}, A^{l}_{B-a}	Upper and lower alarm limits of bus voltage at bus a, respectively	P_{T-L}, Q_{T-L}	Total active and reactive power load, respectively
S_{G-a}, S_{Da}	Apparent power generation and load at bus a, respectively.	S_{xy}	Apparent power flow in the transmission line $x-y$