Synopsis of

A UNIFIED APPROACH FOR SECURITY ASSESSMENT
OF POWER SYSTEMS USING PATTERN CLASSIFIERS

A Thesis
to be submitted by

S. KALYANI

for the award of the degree of

Doctor of Philosophy

Department of Electrical Engineering
Indian Institute of Technology Madras, India.

October 2010
1 Introduction

Power system security has been recognized as an important aspect in planning, design and operation stages since 1920s. Power system networks are forced to operate under highly stressed operating conditions closer to their stability limits in the deregulated environment. Under such conditions, any perturbation could endanger system security and may lead to system collapse. There exists a strong need to develop a fast on-line security monitoring system for analyzing the system security level and forewarning the operators to take necessary preventive actions. 

\textit{Power system security} is the ability of the system to withstand unexpected failures (contingencies) and continue to operate without interruption of supply to consumers.

\textit{Security Assessment} (SA), also referred as Security Evaluation, determines the robustness of the system (security level) to a set of preselected contingencies in its present or future state. It is the analysis performed to determine whether, and to what extent, a power system is reasonably safe from serious interference to its operation. A power system may face contingency conditions like outage of a generating unit, outage of a transmission line, sudden increase in demand, loss of a transformer, a sudden three phase short circuit, etc. Although many such contingencies can occur, only those having a high probability of occurrence are to be considered and such contingencies are known as credible contingencies. A set of most probable (credible) contingencies needs to be first specified for security analysis.

2 Motivation

Traditional method of security evaluation involves numerical solution of nonlinear load flow equations and transient stability analysis with detailed machine modeling for all credible contingencies. This approach, however, requires enormous computation time and found infeasible for real time security analysis of large scale power networks. This necessitates the need for an effective method to evaluate the security status using real time data in a short period of time.
In recent years, many techniques like multilayer feed forward network [1], self-organizing feature map [2], fuzzy logic combined with neural network [3] have been proposed to overcome the limitations of the traditional method. The design procedure of these schemes are found highly system dependent and lacking generalization ability. In early days, attempts were made to exploit pattern recognition techniques [4] for the security assessment problem, where the major issue in the design of an efficient pattern recognition system is to devise a suitable feature selection method and classifier model. However, the existing pattern recognition techniques applied to security evaluation lack the selection of good input features and a classification model with good generalization. These factors (feature selection and classifier model) motivated the search for a computationally efficient, cost effective, pattern recognition scheme with a good classification accuracy and a high speed of assessment.

3 Objectives and Scope

The main objectives identified in this work are:

1. Design of an efficient and reliable pattern classifier system for security assessment of power system networks.
2. Realization of complete security of power systems by performing security assessment and classification in three modes - static, transient and dynamic.
3. Feasibility and applicability of the pattern classifier system for on-line security monitoring and evaluation.

The scope of the present work is limited to static, transient and dynamic security assessment and classification. The list of credible contingencies used for the simulation study in the present work includes only the increase in load demand, single line outages and three phase balanced faults on transmission lines.

4 Description of the Research Work

*Security* is defined as the ability of the power system to remain in a secure state under contingent condition [5]. Security assessment involves estimation of the relative security level of the
current operating condition of the system using available data measurements. The task of security assessment in the present work is performed in three modes - static, transient and dynamic, as shown in Fig. 1. The former characterizes the steady state behavior of the system under a specified contingency, while the transient security deals with evaluating rotor angle oscillations under a transient disturbance. Dynamic security deals with the long term behavior from the instant the system is transiently secure to the instant it reaches steady state. All the three studies need to be sequentially performed on-line, with dynamic security being more complex and difficult than static and transient securities. In case of insecurity in any mode of assessment, an alarm is signaled for the operator to take an appropriate remedial action.

![Diagram of Modes of Security Assessment Process]

**Fig. 1: Modes of security assessment process**

### 4.1 Static Security Assessment

Static security is the ability of a power system to reach a steady state operating point without violating the system operating constraints following a contingency [6]. The violations of thermal limits of transmission lines and bus voltage limits are the main concerns for static security analysis. In conventional practice, Static Security Assessment (SSA) is performed by analytically modeling the network and solving the algebraic load flow equations repeatedly for all prescribed outages, one at a time [7]. This traditional approach involving huge number of sim-
ulations is computationally intensive. The present work defines a term called *Static Security Index* (SSI) for assessing the static security level of a given system operating condition following a contingency. The SSI is computed by calculating the Line Overload Index (LOI) for each branch and Voltage Deviation Index (VDI) for each bus.

### 4.2 Transient Security Assessment

Transient Security Assessment (TSA) consists of determining whether the system oscillations, following the occurrence of a fault or a large disturbance from a contingency set, will cause loss of synchronism among the system generators [8]. It pertains to the rotor angle stability of the power system. Rotor angle stability deals with the ability of the system to remain in synchronism following a major disturbance.

A direct method of transient stability analysis using the classical machine model called Transient Energy Function (TEF) method [9] is used to determine the transient security level. The transient security level is defined based on the computation of a term called *Transient Security Index* (TSI) for a given system operating condition and a specified disturbance. The TEF method involves calculation of two energies: system transient energy at the fault clearing instant and critical energy. Transient energy is the excess energy possessed by the system at the instant of fault clearing, that must be absorbed by the network for stability to be maintained. Critical energy indicates the maximum capacity of system to absorb the accumulated energy during disturbance.

### 4.3 Dynamic Security Assessment

Dynamic Security Assessment (DSA) determines the capability of the system to withstand all credible contingencies, taking into considerations the detailed dynamic characteristics of the system. The system is said to be dynamically secure, if all of its synchronous machines maintain synchronism for a long duration, after it has been found to be transiently secure. It
is a long term stability phenomenon with a time frame of study of the order of few seconds to minutes [10]. DSA requires a detailed modeling of the power system components describing the dynamics of machines and their control elements.

The dynamic behavior of machines represented by two-axis model, exciters by IEEE Type DC1A model, steam turbines and speed governors alone are incorporated [11] in this work. The dynamics of boilers and load frequency controllers is not considered. A direct method of time domain simulation called simultaneous method, where all system dynamic equations are numerically integrated, is adopted. The dynamic security level is defined based on the computation of a term called Dynamic Security Index (DSI), which in turn depends on the calculation of Critical Clearing Time (CCT) for a specified transient disturbance.

5 Security Classifier Model

This thesis work proposes a pattern classifier model for on-line security assessment and classification. Fig. 2 depicts the basic block diagram of the proposed approach of security evaluation and classification using pattern recognition approach. There are two modes of process: off-line and on-line. The off-line process designs a suitable and efficient pattern classifier system for the mode of security assessment under study (SSA/TSA/DSA). The on-line process evaluates and classifies the system operating condition based on the designed pattern classifier system.

Fig. 2: Block diagram of unified scheme of security classifier
5.1 Off-line Process

As seen from Fig. 2, off-line process comprises of two blocks - Data generation and Classification scheme. The generated data samples are preprocessed (normalized) to avoid numerical difficulties in calculation and to prevent domination of one attribute over the other. Based on the normalized data patterns, the classifier system is designed. The feature selection block reduces the huge dimension of pattern vector. The classifier design block uses a suitable learning algorithm and develops the classifier model based on a training data set. The trained classifier model is evaluated for test samples and its performance studied.

5.1.1 Data Generation

The success of any pattern recognition system relies on a good training set. This set must adequately represent the entire range of power system operating states [12]. Data patterns, in this work, are generated by an extensive off-line simulation work. The off-line simulation procedure adopted for each mode of security assessment process is shown in Fig. 3. Each

Fig. 3: Data generation process for different modes of security classification

pattern is characterized by a number of static and dynamic attributes, forming the components of pattern vector X. By computing the security index, each pattern is labeled or classified as
belonging to one of the four classes - Secure, Critically Secure, Insecure and Highly Insecure as shown in Table 1. The security index computed for each mode of security assessment is a percentage measure taking value in the range of 0 to 100. Higher the value of the security index, more severe is the system security level. Based on this idea and a through inspection, the cut off values for these indices corresponding to each class label have been fixed. Data samples generated are randomly split for training and testing process in proportion of 75% and 25% respectively. The list of attributes used in the pattern vector for static, transient and dynamic security evaluation are listed below.

\[
X_{SSA} = \{ |V|_i, \theta_i, S_{Gi}, S_{Li}, S_{ij} \}
\]
\[
X_{TSA} = \{ |V|_i, \theta_i, S_{Gi}, S_{Li}, P_{mk}, \delta^0_k, \delta^{cl}_k, \omega^0_k \}
\]
\[
X_{DSA} = \{|V|_i, \theta_i, S_{Gi}, S_{Li}, \delta^0_k, \omega^0_k, E'_qk, E'_dk, E'_fkd, T_{mk}, \delta^{cl}_k, \omega^{cl}_k, E'_{qk}^{cl}, E'_{dk}^{cl}, E'_{fkd}^{cl}, T_{mk}^{cl} \}
\]

<table>
<thead>
<tr>
<th>Class Category/Label</th>
<th>SSA</th>
<th>TSA</th>
<th>DSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class A: Secure</td>
<td>$SSI = 0$</td>
<td>$TSI = 0$</td>
<td>$DSI = 0$</td>
</tr>
<tr>
<td>Class B: Critically Secure</td>
<td>$SSI &gt; 0 &amp; SSI \leq 5$</td>
<td>$TSI &gt; 0 &amp; TSI \leq 20$</td>
<td>$DSI &gt; 0 &amp; DSI \leq 20$</td>
</tr>
<tr>
<td>Class C: Insecure</td>
<td>$SSI &gt; 5 &amp; SSI \leq 15$</td>
<td>$TSI &gt; 20 &amp; TSI \leq 50$</td>
<td>$DSI &gt; 20 &amp; DSI \leq 60$</td>
</tr>
<tr>
<td>Class D: Highly Insecure</td>
<td>$SSI &gt; 15$</td>
<td>$TSI &gt; 50$</td>
<td>$DSI &gt; 60$</td>
</tr>
</tbody>
</table>

The violations of thermal limits of transmission lines and bus voltage magnitude limits are the main concerns in static security analysis. The Static Security Index (SSI) used in labeling the static security status, shown in Table 1, is categorized based on the evaluation of line overload constraint and voltage limiting constraint for different operating scenarios. The multi-class labels of TSA with different ranges of Transient Security Index (TSI) is decided upon by computing the transient energy level and critical energy level for a specified disturbance set simulated under various static secure operating conditions. In case of DSA problem, the Dynamic Security Index (DSI) is evaluated by finding the critical clearing time (maximum allowable time for clearing a fault without losing dynamic stability) for the disturbance set identified transient
secure and operating conditions identified static secure and then categorized into different class labels by examining the level of dynamic security using the computed DSI.

### 5.1.2 Classification Scheme

#### Feature Selection

Feature selection, a form of dimensionality reduction, is of considerable importance in classification problems. Feature Selection (FS) is the process of selecting a subset of pattern attributes called ‘features’, removing the redundant and irrelevant variables for building robust learning models [13]. The selected feature variables form the components of a vector called feature vector \( Z \). A simple and quick procedure called *Sequential Forward Selection* (SFS), a wrapper model, is identified as a suitable FS method for the security assessment problem addressed herein. This decision was arrived by studying the performance of different feature selection methods like T-test, Chi-squared test, Pearson’s Correlation Coefficient (PCC), Relief algorithm, SFS, Genetic Algorithm based FS (GAFS) and Decision Tree based FS (DTFS) for the security evaluation problem. Among all the FS methods studied, the SFS method was found to give a better classification accuracy with minimal number of selected attributes (features).

The SFS method used in the present work starts with an empty feature set and creates candidate feature subsets by adding one attribute at a time. For each candidate feature subset, SFS performs a 10-fold cross validation by repeatedly calling the criterion function. The criterion function is a loss measure calculating the number of misclassified observations in the cross validation of each candidate feature subset. This process is continued until the addition of more features yields no further decrease in the criterion function.

#### Classifier Design

Classification is basically a scheme of partitioning the feature space into regions, one region for each category or class label [14]. The classifier represents the boundary between the distinctive
classes of separation. The design of classifier is based on the design (training) set of selected features. There are many training algorithms like least squares, back propagation, linear programming, etc. available to design the classifier [4]. These existing algorithms, although less time consuming, have certain limitations like poor classification accuracy and high misclassification rate, especially when the problem size increases. Support Vector Machine (SVM) has been used in this work for multi-classification task in security assessment model. Although SVM is basically intended for binary classification, the concept of multi-class SVM also exists.

*Multi-class SVM* problems are solved by combination of several binary SVM classifiers [15]. Popular methods available are: (i) One-Versus-All (OVA) method and (ii) One-Versus-One (OVO) method. The former method constructs K SVM models, with class i against all other classes, K being number of distinct classes of the problem. The OVA method, although simple, is computationally expensive and not commonly preferred. The OVO method constructs $K(K - 1)/2$ binary classifiers, each being trained from data belonging to the corresponding two classes only with the number of train data considerably reduced in each training session. The classification in OVO method is performed by a Max-Wins Voting (MWV) strategy. After each of the binary classifiers make its vote, the decision function assigns an instance $x$ to a class having largest number of votes. In case of tie with two classes having identical votes, the one with smallest index is selected. The present work has used OVO method for designing the multi-class SVM classifier for security assessment problem.

Kernel mapping allows SVM models to allow separations even with complex boundaries. Radial Basis Function (RBF) is the kernel mapping function used in the design of SVM model. There are two parameters associated with SVM model designed with RBF kernel - penalty parameter, $C$ and RBF kernel parameter, $\gamma$. The parameter selection is performed by a grid search approach with 5-fold cross-validation [16].
5.2 On-line Process

The off-line process yields a security classifier model for direct on-line implementation. In on-line process, real time measurements of selected features are applied to the designed security classifier model and system security status is accessed, as seen from Fig. 2. On-line application of security classification enables operator to monitor the security status from time to time and providing a warning whenever the system goes to emergency state under severe contingency.

6 Results and Observations

Data generation for the design of pattern classifier system for different modes of security assessment is obtained through off-line simulations as shown detailed in Fig. 3. We have considered different operating scenarios by varying the system active load and generation from 50% to 200%, in steps of 5%, of base case and distributing among all buses in proportion to their respective base value. All contingencies in the contingency list are simulated one at a time for each load generation pattern. The contingency list in SSA consists of single line outages and that for TSA and DSA consists of three phase balanced faults on transmission lines, one at a time. The security level of each operating scenario is determined based on the computation of appropriate security index and the class labeling of each data pattern is performed as shown in Table 1. A small scale dynamic New England 39 bus system and a large scale IEEE 118 bus system are considered for the simulation study. The results of data generation and feature selection process for SSA, TSA and DSA problems is shown in Table 2. The figures shown in brackets in Table 2 indicates the number of samples randomly chosen for training and testing processes.

After extracting the relevant features for classifier design, the security function is designed using different pattern classifiers and their performance are evaluated. The pattern classifiers used in the simulation work includes k-nearest neighbor, naive bayes, least squares, neural...
Table 2: Data generation and feature selection of different security assessment problems

<table>
<thead>
<tr>
<th></th>
<th>SSA</th>
<th>TSA</th>
<th>DSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>NE 39 Bus</td>
<td>NE 39 Bus</td>
<td>NE 39 Bus</td>
<td>NE 39 Bus</td>
</tr>
<tr>
<td>IEEE 118 Bus</td>
<td>IEEE 118 Bus</td>
<td>IEEE 118 Bus</td>
<td>IEEE 118 Bus</td>
</tr>
<tr>
<td><strong>Total Operating Cases</strong></td>
<td>548 (410+138)</td>
<td>3537 (2652+885)</td>
<td>884 (663+221)</td>
</tr>
<tr>
<td><strong>Class A: Secure</strong></td>
<td>87 (66+21)</td>
<td>174 (130+44)</td>
<td>736 (551+185)</td>
</tr>
<tr>
<td><strong>Class B: Critically Secure</strong></td>
<td>275 (208+67)</td>
<td>2391 (1797+594)</td>
<td>38 (28+10)</td>
</tr>
<tr>
<td><strong>Class C: Insecure</strong></td>
<td>158 (117+41)</td>
<td>344 (254+90)</td>
<td>43 (30+13)</td>
</tr>
<tr>
<td><strong>Class D: Highly Insecure</strong></td>
<td>28 (19+9)</td>
<td>628 (471+157)</td>
<td>67 (54+13)</td>
</tr>
<tr>
<td><strong>No. of Pattern Attributes</strong></td>
<td>153</td>
<td>568</td>
<td>147</td>
</tr>
<tr>
<td><strong>No. of Features Selected</strong></td>
<td>17</td>
<td>52</td>
<td>26</td>
</tr>
</tbody>
</table>

Network architectures, decision trees, support vector machines and clustering techniques. Two performance measures, viz., Classification Accuracy \((CA)\) and Misclassification for a class \(K (MC_K)\) as given by (1) and (2) respectively, are computed to evaluate the performance of different classifier algorithms on test data samples. The classification results obtained by few important pattern classifiers for all modes of security assessment is shown in Table 3. The entries in brackets under each percentage measure in Table 3 shows the numerical values of numerator and denominator term as given by Eq. 1 and Eq. 2.

\[
CA(\%) = \frac{\text{No. of samples classified correctly}}{\text{Total No. of samples in data set}} \times 100 \tag{1}
\]

\[
MC_K(\%) = \frac{\text{No. of misclassification in class } K}{\text{Total No. of samples belonging to class } K} \times 100 \tag{2}
\]

It can be observed from the results of classification shown in Table 3 for different modes of security assessment that SVM classifier gives a relatively better performance compared to other pattern classifiers. The security classification problem aims to minimize the misclassification in class C and class D, as they indicate the wrong classification of highly insecure states, leading to a severe blackout. Observation of the results of \(MC_A\) in SSA, a high fluctuating performance occurs for different pattern classifiers due to less number of samples belonging to Class B.
Table 3: Performance of pattern classifiers for different security assessment problems

<table>
<thead>
<tr>
<th>Measures ↓</th>
<th>NE 39 Bus system</th>
<th>IEEE 118 Bus system</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MLS</td>
<td>PNN</td>
</tr>
<tr>
<td><strong>Total number of samples evaluated:</strong></td>
<td>138</td>
<td>885</td>
</tr>
<tr>
<td><strong>CA (%)</strong></td>
<td>75.36</td>
<td>85.51</td>
</tr>
<tr>
<td><strong>MC_A (%)</strong></td>
<td>80.95</td>
<td>19.05</td>
</tr>
<tr>
<td><strong>MC_B (%)</strong></td>
<td>2.99</td>
<td>5.97</td>
</tr>
<tr>
<td><strong>MC_C (%)</strong></td>
<td>34.15</td>
<td>21.95</td>
</tr>
<tr>
<td></td>
<td>(144/41)</td>
<td>(9/41)</td>
</tr>
<tr>
<td><strong>MC_D (%)</strong></td>
<td>11.11</td>
<td>33.33</td>
</tr>
<tr>
<td><strong>Time (s)</strong></td>
<td>0.12</td>
<td>0.07</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Measures ↓</th>
<th>NE 39 Bus system</th>
<th>IEEE 118 Bus system</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MLS</td>
<td>PNN</td>
</tr>
<tr>
<td><strong>Total number of samples evaluated:</strong></td>
<td>221</td>
<td>1190</td>
</tr>
<tr>
<td><strong>CA (%)</strong></td>
<td>80.09</td>
<td>83.71</td>
</tr>
<tr>
<td></td>
<td>(177/221)</td>
<td>(185/221)</td>
</tr>
<tr>
<td><strong>MC_A (%)</strong></td>
<td>9.73</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>(18/185)</td>
<td>(0/185)</td>
</tr>
<tr>
<td><strong>MC_B (%)</strong></td>
<td>20.00</td>
<td>100.0</td>
</tr>
<tr>
<td></td>
<td>(2/10)</td>
<td>(10/10)</td>
</tr>
<tr>
<td><strong>MC_C (%)</strong></td>
<td>84.62</td>
<td>100.0</td>
</tr>
<tr>
<td><strong>MC_D (%)</strong></td>
<td>100.0</td>
<td>100.0</td>
</tr>
<tr>
<td><strong>Time (s)</strong></td>
<td>0.04</td>
<td>0.31</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Measures ↓</th>
<th>NE 39 Bus system</th>
<th>IEEE 118 Bus system</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MLS</td>
<td>PNN</td>
</tr>
<tr>
<td><strong>Total number of samples evaluated:</strong></td>
<td>184</td>
<td>1168</td>
</tr>
<tr>
<td><strong>CA (%)</strong></td>
<td>48.37</td>
<td>22.83</td>
</tr>
<tr>
<td></td>
<td>(89/184)</td>
<td>(42/184)</td>
</tr>
<tr>
<td><strong>MC_A (%)</strong></td>
<td>78.57</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>(33/42)</td>
<td>(0/42)</td>
</tr>
<tr>
<td><strong>MC_B (%)</strong></td>
<td>42.86</td>
<td>100.0</td>
</tr>
<tr>
<td></td>
<td>(7/7)</td>
<td>(7/7)</td>
</tr>
<tr>
<td><strong>MC_C (%)</strong></td>
<td>38.75</td>
<td>100.0</td>
</tr>
<tr>
<td><strong>MC_D (%)</strong></td>
<td>50.91</td>
<td>100.0</td>
</tr>
<tr>
<td></td>
<td>(28/55)</td>
<td>(55/55)</td>
</tr>
<tr>
<td><strong>Time (s)</strong></td>
<td>0.03</td>
<td>0.08</td>
</tr>
</tbody>
</table>

NA: Not Applicable (Samples in test set belonging to Class B is zero)
MLS: Method of Least Squares, PNN: Probabilistic Neural Network
DTC: Decision Tree Classifier, ELM: Extreme Learning Machine, SVM: Support Vector Machine
CA: Classification Accuracy, MC_k: Misclassification rate in Class k

12 / 16
category compared to samples in other classes. The misclassification rate (Class B, Class C and Class D) in case of TSA result for IEEE 118 bus system is found to be 100% for all pattern classifiers due to the fact of only few samples belonging to Class B, Class C and Class D as seen from Table 1 and all of which has been wrongly classified. A combined requirement of high classification accuracy, less misclassification rate in Class C and Class D and less evaluation time is found to be achieved by the SVM classifier compared to other pattern classifiers for all modes of security assessment.

A further observation of Table 3 shows that SVM classifiers take very less time of the order of milliseconds for evaluating a set of test samples. In real time application, only one sample needs to be accessed for security status at a particular instant, still reducing the classification time requirement of developed SVM model. Thus, the SVM based security classifier model, capable of accessing the security level in less time with high accuracy, is found to be suitable for on-line implementation. The real time measurements of only selected features are used in the on-line security classifier system. Such an application will allow the operator to monitor the system security status from time to time, and take appropriate control actions, whenever needed.

7 Conclusions

The following are the important conclusions arising out of this work:

1. An efficient and reliable pattern classifier system for security assessment of power systems is developed.

2. A unified classification approach for static, transient and dynamic security evaluation is proposed to give a better indication of system security level to the operator.

3. The proposed security classifier model developed is suitable for implementation in real time.
REFERENCES


8 Proposed Contents of the Thesis

1. INTRODUCTION
   1.1 Power System Security
   1.2 Motivation
   1.3 Objectives and Scope of Work
   1.4 Organization of the Thesis

2. POWER SYSTEM SECURITY ASSESSMENT
   2.1 Introduction
   2.2 Modes of Security Assessment
   2.3 Survey of Related Literature
   2.4 Overview of the Proposed Approach

3. PATTERN RECOGNITION APPROACH
   3.1 Introduction
   3.2 Data Generation and Preprocessing
   3.3 Feature Selection
   3.4 Classifier Design

4. STATIC SECURITY ASSESSMENT CLASSIFIER
   4.1 Introduction
   4.2 Test Systems
   4.3 Binary and Multi-Classification Based SSA
   4.4 Improving Performance of SVM Model

5. TRANSIENT SECURITY ASSESSMENT CLASSIFIER
   5.1 Introduction
   5.2 Test Systems
   5.3 Binary and Multi-Classification Based TSA

6. DYNAMIC SECURITY ASSESSMENT CLASSIFIER
   6.1 Introduction
   6.2 Test Systems
   6.3 Binary and Multi-Classification Based DSA

7. ON-LINE IMPLEMENTATION
   7.1 Introduction
   7.2 On-line Implementation of Security Classifier System

8. CONCLUSIONS
   8.1 Important Conclusions
   8.2 Contributions of the Work
   8.3 Scope for Future Work
9 List of Publications based on the Research Work

Journals


Conference Proceedings


