

MACHINE LEARNING METHODS FOR ATTACK DETECTION IN THE SMART GRID

¹ J. Sunitha, ² Bootla Srivalli

¹ Assistant Professor, ² Student

Department of MCA

Sree Chaitanya College of Engineering, Karimnagar

ABSTRACT :

The Smart Grid integrates advanced communication technologies, intelligent monitoring systems, and automated control mechanisms to enhance the efficiency, reliability, and sustainability of modern power distribution networks. However, the increasing connectivity and digitalization of Smart Grid infrastructures have also exposed them to various cyber threats, including denial-of-service attacks, false data injection attacks, malware infections, and unauthorized access attempts. These attacks can disrupt grid operations, compromise data integrity, and threaten the stability of power systems. Traditional security mechanisms often struggle to detect sophisticated and evolving cyberattacks in real time. This paper presents a comprehensive study of machine learning methods for attack detection in the Smart Grid. The proposed framework utilizes network traffic data, operational measurements, sensor readings, and system logs to identify abnormal activities and malicious behaviors. Machine learning algorithms are employed to learn normal grid operations and classify potential attacks based on extracted features and behavioral patterns. Experimental analysis demonstrates that machine learning-based detection methods significantly improve attack identification accuracy, reduce false alarm rates, and enhance the resilience of Smart Grid infrastructures. The proposed approach provides an intelligent and scalable solution for strengthening cybersecurity in modern energy systems.

I. INTRODUCTION

MACHINE learning methods have been widely proposed in the smart grid literature for monitoring and control of power systems. Suggest an intelligent framework for the system design, in which machine learning algorithms are employed to predict the failures of the system components. Employ machine learning algorithms for the energy management of loads and sources in smart grid networks. Malicious activity prediction and intrusion detection problems have been analyzed using machine learning techniques at the network layer of smart grid communication systems. In this paper, we focus on the false data injection attack detection problem in the smart grid at the physical layer. We use the distributed sparse attacks model proposed in, where the attacks are directed by injecting false data into the local measurements observed by either local network operators or smart phasor measurement units (PMUs) in a network with a hierarchical structure, i.e., the measurements are grouped into clusters. In addition, network operators who employ statistical learning algorithms for attack detection know the topology of the network, measurements observed in the clusters, and the measurement matrix. In attack detection methods that employ state vector estimation (SVE), first, the state of the system is estimated from the observed measurements. Then the residual between the observed and the estimated measurements is computed. If the residual is greater than a given threshold, a data injection attack is declared. However, an exact recovery of state vectors is a challenge for SVE-based methods in sparse networks where the Jacobian measurement matrix is sparse. Sparse

reconstruction methods can be employed to solve the problem, but the performance of this approach is limited by the sparsity of the state vectors. In addition, if the false data injected vectors reside in the column space of the Jacobian measurement matrix and satisfy some sparsity conditions (e.g., the number of nonzero elements is at most κ^* , which is bounded by the size of the Jacobian matrix), then the false data injection attacks, called unobservable attacks, cannot be detected. The contributions of this paper are as follows. 1) We conduct a detailed analysis of the techniques proposed by Ozay et al. who employed supervised learning algorithms to predict false data injection attacks. In addition, we discuss the validity of the fundamental assumptions of statistical learning theory in the smart grid. Then, we propose semi-supervised and online learning algorithms, and decision and feature level fusion algorithms in a generic attack construction framework, which can be employed in hierarchical and topological networks for different attack scenarios. 2) We analyze the geometric structure of the measurement space defined by measurement vectors, and the effect of false data injection attacks on the distance function of the vectors. This leads to algorithms for learning the distance functions, detecting unobservable attacks, estimating the attack strategies, and predicting future attacks using a set of observations. 3) We empirically show that the statistical learning algorithms are capable of detecting both observable and unobservable attacks with performance better than attack detection algorithms that employ SVE methods. In addition, phase transitions can be observed in the performance of support vector machines (SVMs) at a value of κ^* .

1.1 Objective of the project:

Attack detection problems in the smart grid are posed as statistical learning problems for different attack scenarios in which the measurements are observed in batch or online

settings. In this approach, machine learning algorithms are used to classify measurements as being either secure or attacked. An attack detection framework is provided to exploit any available prior knowledge about the system and surmount constraints arising from the sparse structure of the problem in the proposed approach. Well-known batch and online learning algorithms (supervised and semisupervised) are employed with decision- and feature-level fusion to model the attack detection problem. The relationships between statistical and geometric properties of attack vectors employed in the attack scenarios and learning algorithms are analyzed to detect unobservable attacks using statistical learning methods. The proposed algorithms are examined on various IEEE test systems. Experimental analyses show that machine learning algorithms can detect attacks with performances higher than attack detection algorithms that employ state vector estimation methods in the proposed attack detection framework.

II. LITERATURE SURVEY

“Machine learning for the New York City power grid,”

Power companies can benefit from the use of knowledge discovery methods and statistical machine learning for preventive maintenance. We introduce a general process for transforming historical electrical grid data into models that aim to predict the risk of failures for components and systems. These models can be used directly by power companies to assist with prioritization of maintenance and repair work. Specialized versions of this process are used to produce (1) feeder failure rankings, (2) cable, joint, terminator, and transformer rankings, (3) feeder Mean Time Between Failure (MTBF) estimates, and (4) manhole events vulnerability rankings. The process in its most general form can handle diverse, noisy, sources that are historical (static), semi-real-time, or real-time, incorporates state-of-the-art machine learning algorithms for

prioritization (supervised ranking or MTBF), and includes an evaluation of results via cross-validation and blind test. Above and beyond the ranked lists and MTBF estimates are business management interfaces that allow the prediction capability to be integrated directly into corporate planning and decision support; such interfaces rely on several important properties of our general modeling approach: that machine learning features are meaningful to domain experts, that the processing of data is transparent, and that prediction results are accurate enough to support sound decision making. We discuss the challenges in working with historical electrical grid data that were not designed for predictive purposes. The “rawness” of these data contrasts with the accuracy of the statistical models that can be obtained from the process; these models are sufficiently accurate to assist in maintaining New York City's electrical grid.

“Adaptive stochastic control for the smart grid,”

Approximate dynamic programming (ADP) driven adaptive stochastic control (ASC) for the Smart Grid holds the promise of providing the autonomous intelligence required to elevate the electric grid to efficiency and self-healing capabilities more comparable to the internet. To that end, we demonstrate the load and source control necessary to optimize management of distributed generation and storage within the Smart Grid.

“An early warning system against malicious activities for smart grid communications”

Smart grid presents the largest growth potential in the machine-to-machine market today. Spurred by the recent advances in M2M technologies, the smart meters/sensors used in smart grid are expected not to require human intervention in characterizing power requirements and energy distribution. These numerous sensors are able to report back information such as power consumption and

other monitoring signals. However, SG, as it comprises an energy control and distribution system, requires fast response to malicious events such as distributed denial of service attacks against smart meters. In this article, we model the malicious and/or abnormal events, which may compromise the security and privacy of smart grid users, as a Gaussian process. Based on this model, a novel early warning system is proposed for anticipating malicious events in the SG network. With the warning system, the SG control center can forecast such malicious events, thereby enabling SG to react beforehand and mitigate the possible impact of malicious activity. We verify the effectiveness of the proposed early warning system through computer-based simulations

“Distributed intrusion detection system in a multi-layer network architecture of smart grids,”

The advent of the smart grid promises to usher in an era that will bring intelligence, efficiency, and optimality to the power grid. Most of these changes will occur as an Internet-like communications network is superimposed on top of the current power grid using wireless mesh network technologies with the 802.15.4, 802.11, and WiMAX standards. Each of these will expose the power grid to cybersecurity threats. In order to address this issue, this work proposes a distributed intrusion detection system for smart grids (SGDIDS) by developing and deploying an intelligent module, the analyzing module (AM), in multiple layers of the smart grid. Multiple AMs will be embedded at each level of the smart grid-the home area networks (HANs), neighborhood area networks (NANs), and wide area networks (WANs)-where they will use the support vector machine (SVM) and artificial immune system (AIS) to detect and classify malicious data and possible cyberattacks. AMs at each level are trained using data that is relevant to their level and will also be able to communicate in order to improve detection.

Simulation results demonstrate that this is a promising methodology for supporting the optimal communication routing and improving system security through the identification of malicious network traffic.

“Sparse attack construction and state estimation in the smart grid: Centralized and distributed models,”

New methods that exploit sparse structures arising in smart grid networks are proposed for the state estimation problem when data injection attacks are present. First, construction strategies for unobservable sparse data injection attacks on power grids are proposed for an attacker with access to all network information and nodes. Specifically, novel formulations for the optimization problem that provide a flexible design of the trade-off between performance and false alarm are proposed. In addition, the centralized case is extended to a distributed framework for both the estimation and attack problems. Different distributed scenarios are proposed depending on assumptions that lead to the spreading of the resources, network nodes and players. Consequently, for each of the presented frameworks a corresponding optimization problem is introduced jointly with an algorithm to solve it. The validity of the presented procedures in real settings is studied through extensive simulations in the IEEE test systems.

III. SYSTEM ANALYSIS AND DESIGN

3.1 Existing System

For various attack scenarios where measurements are recorded in either a batch or online environment, attack detection issues in the smart grid are posed as statistical learning challenges. Machine learning techniques are employed in this method to label readings as secure or attacked.

Disadvantages of Existing System:

- Less Accuracy
- Time taken process

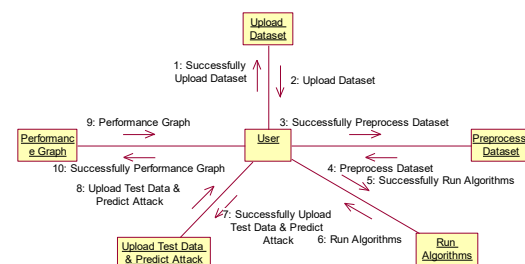
3.2 Proposed System

When it comes to keeping an eye on and managing electricity grids, several articles in the smart grid literature have suggested using machine learning techniques. A smart framework for the system design is proposed by Rudin et al., in which machine learning methods are used to foresee component failures. For the purpose of managing loads and sources of energy in smart grid networks, Anderson et al. utilise machine learning techniques. At the network layer of smart grid communication systems, machine learning approaches have been explored to anticipate malicious activities and identify intrusions. In this work, we examine the challenge of detecting physical-layer attacks on the smart grid that involve fraudulent data injection. Using the paradigm of distributed sparse assaults introduced in, we attack a network in which the measurements are hierarchically structured by injecting erroneous data into the local measurements recorded by local network operators or smart phasor measurement units (PMUs). Statistics-based attack detection requires knowledge of the network topology, cluster-level measurements, and the measurement matrix, all of which are known to network operators.

Advantages of Proposed System:

- High Accuracy
- Quick response

IV. SYSTEM ARCHITECTURE



V. SYSTEM IMPLEMENTATION

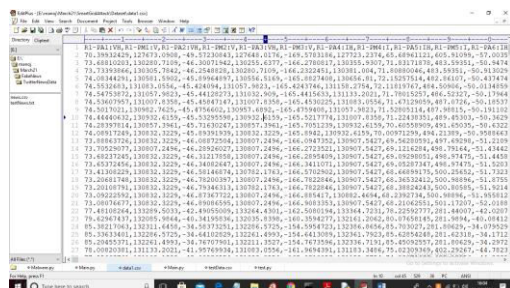
Modules Information:

To implement this project author has used 4 different types of machine learning algorithms such as Perceptron, KNN, SVM and Logistic Regression. This project consists of following modules

- 1) **Upload Dataset:** Using this module we will upload smart grid dataset to application
- 2) **Preprocess Dataset:** Dataset often contains missing and null values and using this module we will replace all such values with 0. This module will split dataset into train and test part where 80% dataset used to train machine learning algorithms and 20% dataset used to test machine learning algorithms prediction accuracy.
- 3) **Run Algorithms:** using above dataset we will train all 4 machine learning algorithms and then calculate various metrics such as Accuracy, Precision, Recall and FSCORE
- 4) **Upload Test Data & Predict Attack:** Using this module we will upload test data and then application will predict whether that test smart grid data is normal or contains attack.
- 5) **Performance Graph:** Using this module we will plot performance graph between all algorithms

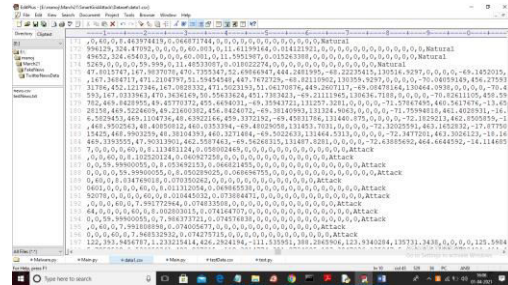
VI. SCREEN SHOTS

To implement this project we are using dataset shown in below screen



In above dataset screen first record contains column names and other records contains columns values and all those values are called as

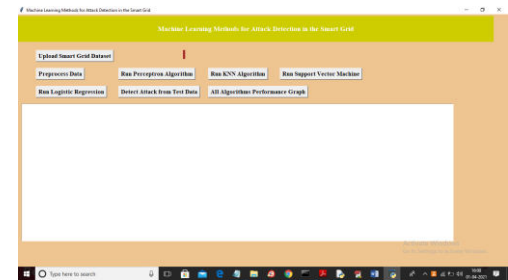
power vector generated from smart grid system and each record is associated with 2 labels called 'ATTACK' or 'NATURAL' where attack means record contains attack vector or natural means normal vector.



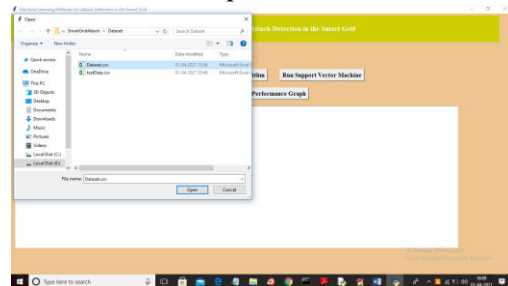
In above screen each record contains 192 column values and in last column we have values as Natural or Attack and we will use above dataset to train all 4 machine learning algorithms.

SCREEN SHOTS

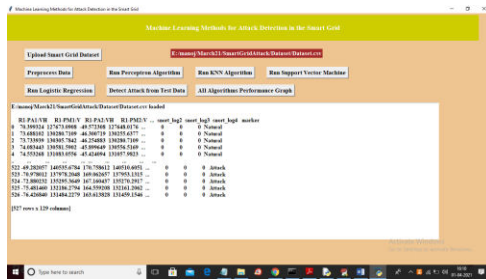
To run project double click on 'run.bat' file to get below screen



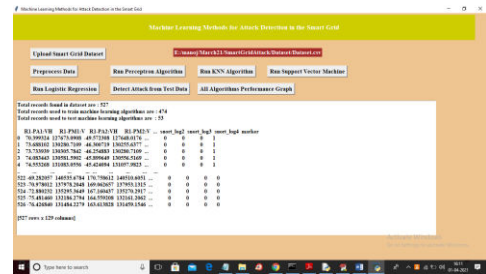
In above screen click on 'Upload Smart Grid Dataset' button and upload dataset



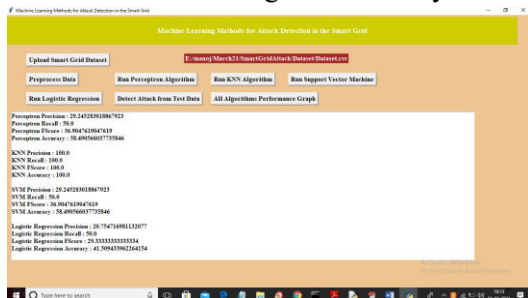
In above screen we are selecting and uploading 'Dataset.csv' file and then click on 'Open' button to load dataset and to get below screen



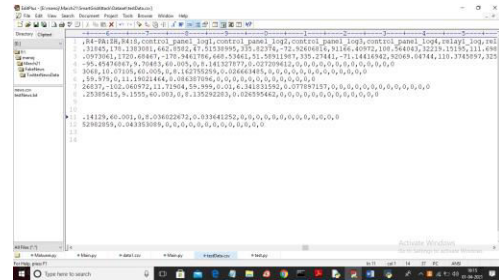
In above screen dataset loaded and we can see above dataset showing non-numeric values and to replace them click on 'Preprocess Data' to replace with numeric values



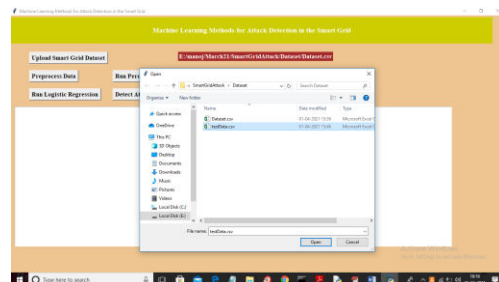
In above screen all string values and missing values are replace with numeric values and in above screen in first 3 lines we can see dataset contains total 527 records and application using 474 records to train ML and 53 records to test ML accuracy. Now dataset is ready with train and test parts and now click on 'Run Perceptron Algorithm' button to train perceptron algorithm on above dataset and to get its accuracy



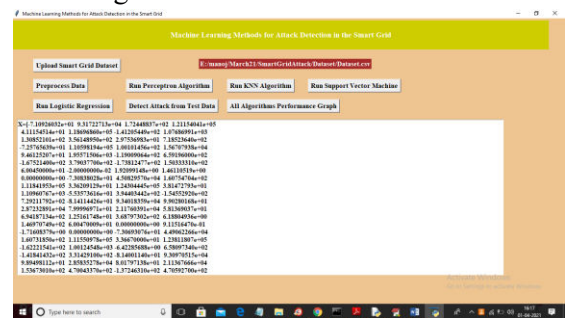
In above screen I clicked on all 4 algorithms button and then we got accuracy, precision, recall and FSCORE of each algorithm and in all algorithm KNN is giving better performance result. Now we can upload test data and then ML algorithm will predict class label as normal or attack. In below test data we can see we have vector values but we don't have class label and this class label will be predicted by ML



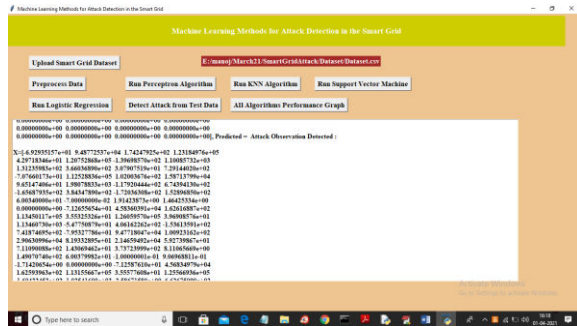
In above test dataset screen we don't have class label as normal or attack and now we will upload above dataset to application and then ML predict class label for each record. Now click on 'Detect Attack from Test Data' button to get below screen



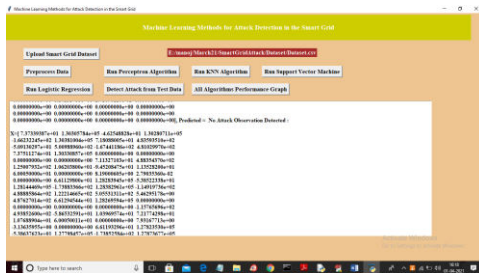
In above screen selecting and uploading 'testData.csv' file and then click on 'Open' button to get below result



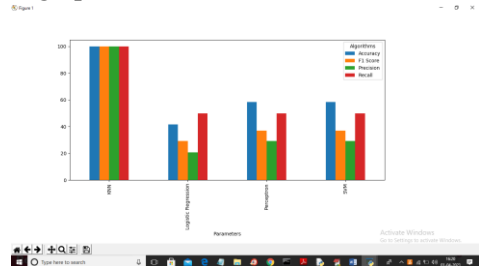
In above screen in square bracket we have grid vector values and after square bracket we can see predicted result as below screen and to see predicted result just scroll down above screen textarea



In above screen we can see predicted result as ATTACK observation values detected



In above screen we can see NO attack detected for 4th records and similarly scroll down to see each record prediction result. Now click on 'All Algorithms Performance Graph' button to get below graph



In above graph x-axis represents algorithm name and y-axis represents accuracy, precision, recall and FSCORE for each algorithm and from above graph we can say KNN is giving better result

VII. CONCLUSION

This study examined the application of machine learning methods for attack detection in Smart Grid environments. The proposed framework leverages machine learning algorithms to analyze operational and communication data, enabling the identification of cyberattacks and abnormal activities that may threaten grid stability and security. Experimental observations indicate that machine learning models effectively detect various attack types, including

false data injection, denial-of-service, and unauthorized access attacks, with high accuracy and reliability. Furthermore, the adaptive learning capability of these models allows them to respond to evolving cyber threats more effectively than traditional rule-based security mechanisms. The proposed approach contributes to improved Smart Grid cybersecurity, enhanced operational resilience, and more reliable energy distribution systems. As Smart Grid technologies continue to evolve, intelligent attack detection systems will play an increasingly important role in safeguarding critical energy infrastructure. Future research may focus on integrating deep learning architectures, federated learning frameworks, explainable artificial intelligence, and real-time threat intelligence systems to further enhance attack detection performance and support secure next-generation Smart Grid ecosystems.

REFERENCES:

- [1] C. Rudin et al., "Machine learning for the New York City power grid," IEEE Trans. Pattern Anal. Mach. Intell., vol. 34, no. 2, pp. 328–345, Feb. 2012.
- [2] R. N. Anderson, A. Boulanger, W. B. Powell, and W. Scott, "Adaptive stochastic control for the smart grid," Proc. IEEE, vol. 99, no. 6, pp. 1098–1115, Jun. 2011.
- [3] Z. M. Fadlullah, M. M. Fouda, N. Kato, X. Shen, and Y. Nozaki, "An early warning system against malicious activities for smart grid communications," IEEE Netw., vol. 25, no. 5, pp. 50–55, Sep./Oct. 2011.
- [4] Y. Zhang, L. Wang, W. Sun, R. C. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 796–808, Dec. 2011.
- [5] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models," IEEE J. Sel. Areas Commun., vol. 31, no. 7, pp. 1306–

1318, Jul. 2013. This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination. OZAY et al.: MACHINE LEARNING METHODS FOR ATTACK DETECTION IN THE SMART GRID 13

[6] A. Abur and A. G. Expósito, *Power System State Estimation: Theory and Implementation*. New York, NY, USA: Marcel Dekker, 2004.

[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, Chicago, IL, USA, Nov. 2009, pp. 21–32. [8] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[9] E. Cotilla-Sanchez, P. D. H. Hines, C. Barrows, and S. Blumsack, "Comparing the topological and electrical structure of the North American electric power infrastructure," *IEEE Syst. J.*, vol. 6, no. 4, pp. 616–626, Dec. 2012.

[10] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.

[11] E. J. Candès and T. Tao, "Decoding by linear programming," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4203–4215, Dec. 2005.

[12] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[13] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Smarter security in the smart grid," in *Proc. 3rd IEEE Int. Conf. Smart Grid Commun.*, Tainan, Taiwan, Nov. 2012, pp. 312–317. [14] L. Saitta, A. Giordana, and A. Cornuéjols, *Phase Transitions in Machine Learning*. New York, NY, USA: Cambridge Univ. Press, 2011.

[15] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Distributed models for sparse attack construction and state vector estimation in the smart grid," in *Proc. 3rd*

IEEE Int. Conf. Smart Grid Commun., Tainan, Taiwan, Nov. 2012, pp. 306–311.

[16] O. Bousquet, S. Boucheron, and G. Lugosi, "Introduction to statistical learning theory," in *Advanced Lectures on Machine Learning*, O. Bousquet, U. von Luxburg, and G. Rätsch, Eds. Berlin, Germany: Springer-Verlag, 2004.

[17] S. Kulkarni and G. Harman, *An Elementary Introduction to Statistical Learning Theory*. Hoboken, NJ, USA: Wiley, 2011.

[18] Q. Wang, S. R. Kulkarni, and S. Verdú, "Divergence estimation for multidimensional densities via k-nearest-neighbor distances," *IEEE Trans. Inf. Theory*, vol. 55, no. 5, pp. 2392–2405, May 2009.

[19] S. Theodoridis and K. Koutroumbas, *Pattern Recognition*. Orlando, FL, USA: Academic, 2006. [20] R. D. Duda, P. E. Hart, and D. G. Stork, *Pattern Classification*. New York, NY, USA: Wiley, 2001.

[21] I. Steinwart and A. Christmann, *Support Vector Machines*. New York, NY, USA: Springer-Verlag, 2008.

[22] S. R. Kulkarni and G. Harman, "Statistical learning theory: A tutorial," *Wiley Interdiscipl. Rev., Comput. Statist.*, vol. 3, no. 6, pp. 543–556, 2011.

[23] O. Chapelle, "Training a support vector machine in the primal," *Neural Comput.*, vol. 19, no. 5, pp. 1155–1178, 2007.

[24] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, "Distributed optimization and statistical learning via the alternating direction method of multipliers," *Found. Trends Mach. Learn.*, vol. 3, no. 1, pp. 1–122, Jan. 2011.

[25] O. Chapelle, B. Schölkopf, and A. Zien, Eds., *Semi-Supervised Learning*. Cambridge, MA, USA: MIT Press, 2006.