An Introductory Review Of Anomaly Detection Methods In Smart Grids

Preethi G[1], Anitha Kumari K[2]
{gpi.dit@psgpolytech.ac.in[1], kak.it@psgtech.ac.in[2] }

Department of Information Technology, PSG College of Technology, Coimbatore[1,2]

Abstract. Cyber Physical systems such as smart grids have the potential to address the future energy crisis. Because of the bidirectional flow of information across various domains in a smart grid, anomaly detection is one of the prime security related challenges. Machine learning models have emerged as one of the prospective artificial intelligence technologies to model supervised and unsupervised data for analysis and prediction. This paper reviews the various anomaly detection schemes in a Smart Grid Infrastructure based on machine learning techniques.

Keywords: Machine learning, Smart Grids, supervised learning, unsupervised learning, Anomaly detection..

1 Introduction

This The Smart Grid (SG) is a distributed power framework that enables the two-way communication of information and energy between the utilities and customers. The infrastructure of the SG encompasses various domains such as bulk generation, distribution, transmission and operations spanning customers and service providers in the energy market [1]. A Smart grid protection system is a subsystem of SG that focuses on protecting the reliability, security and privacy against various anomalies. Anomaly detection involves monitoring the metering, measurement and transmission of energy (and information) leading to identification, localization and prediction of factors leading to failure of a SG. An effective anomaly detection model can successfully bring about reliability, security and privacy of a SG. While government organizations across the world enforce legislations and standards to ensure a safe and reliable SG, technologies like machine learning can actively contribute to the analysis, monitoring and identification of anomalies at various points in a smart grid. Various supervised and unsupervised machine learning based algorithms have been proposed for anomaly detection in SC framework.

In this paper, a broad and discursive survey on the anomaly detection schemes associated with machine learning techniques has been presented. The rest of the paper is organized into the following sections: Section 2 elaborate on the security infrastructure of the SG. Section 3 provides a brief description of the machine learning techniques. Section 4 provides an extensive literature survey on the various machine learning models and schemes for anomaly detection. Section 5 summarizes the conclusion and future directions of research on secure SG.

.

ICCAP 2021, December 07-08, Chennai, India

DOI 10.4108/eai.7-12-2021.2314604

2 SMART GRID SECURITY INFRASTRUCTURE

An understanding of the various domains in an SG infrastructure is paramount to realize the security and privacy requirements with respect to each entity in the domains. The National Institute of Standards and Technology (NIST) [have defined seven major domains of SG and the entities in each domain [2]. Figure 1. illustrates the SG domains based on the NIST model. Unlike the conventional power grid, distributed resources such as solar plants and wind turbines also contribute energy to the SG. In [3], Pallotti.et.al defines the CIA triad of SG security and lists the various security practices to achieve information security in SG. Localized generation and transmission power units called Microgrids can be constructed and coupled with the Macrogrid (the traditional grid) when in excess power requirement. Information and energy are generated and transmitted between various entities across domains in SG. Data collected from entities like smart meters, sensors and Phasor Measurement Units is rigorously monitored by means of Advanced Metering Infrastructure (AMI) and Supervisory Control and Data Acquisition (SCADA) systems facilitate [4].

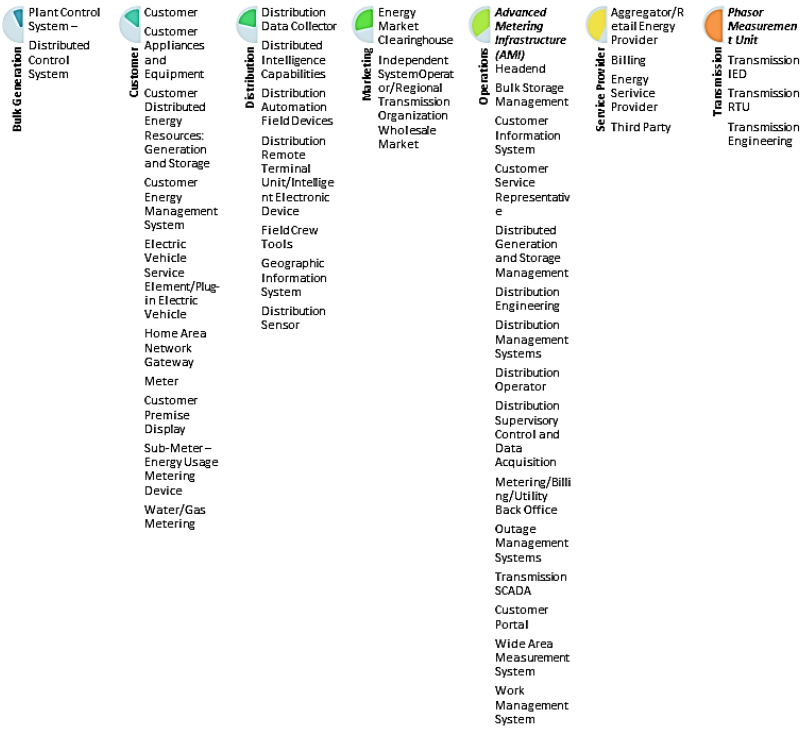

Fig 1. Smart Grid Domains and their Corresponding Entities

Because the SG data is represented in a compatible, transferable and editable format, these entities also have the potential to become the anomaly hotspots. Vulnerable information such as customer's smart meter profile, billing history and network configuration can be exploited if not properly safeguarded. These data, generated at various domains in an SG infrastructure may be exploited by adversaries such as hackers, cyber terrorists, industrial competitors, organized criminal elements, disgruntled and poorly trained employees to create

anomalies. Since the SC ultimately aims at delivering uninterrupted and reliable energy, anomaly detection has become one of the paramount security challenges in SC.

3 SMART GRID SECURITY INFRASTRUCTURE

Machine learning is a pervasive and powerful class of algorithms designed to learn from data, acquire key insights to make efficient classifications and predictions that drive intelligent decision making. Machine learning approaches are commonly distinguished as Supervised, unsupervised, Semi-supervised and Reinforcement based learning models. Supervised learning deals with labeled and structured data. Unsupervised learning deals with unlabeled data. Semi-supervised learning deals with labeled and unlabeled data. Reinforcement learning involves an agent learning actions that maximizes the rewards and minimizes the risks. Figure 2. illustrates the common machine learning algorithms under each category.

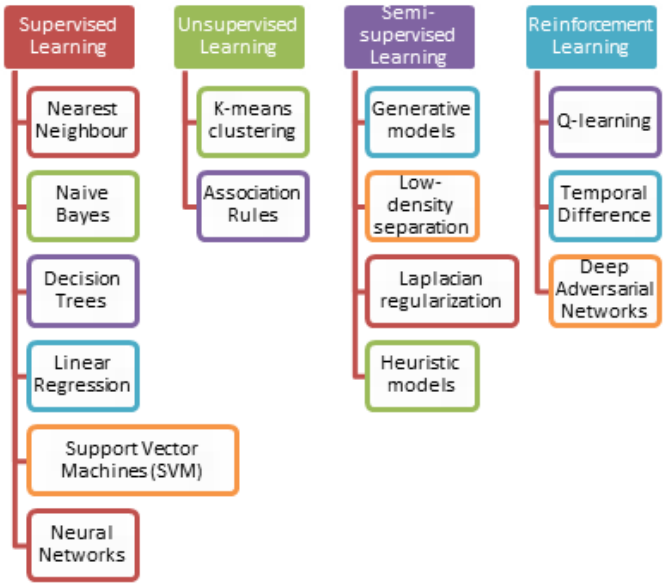

Fig.2 Common Categories of Machine Learning Algorithms

4 LITERATURE SURVEY ON MACHINE LEARNING (ML) APPROACHES FOR ANOMALY DETECTION IN SMART GRID

With respect to anomaly detection, machine learning algorithms are adaptive in handling real time data and give a better performance in detecting malicious behavioral patterns. This section presents the chronological review on the various anomaly detection methods proposed for a smart grid framework based on the various parameters of the energy data.

Kher et.al.in [5][6] proposed a sensor network-based hybrid framework for SG monitoring. The two-layer mesh topology routing protocol consists of local clusters with fixed number of heads at lower level and cluster heads at each node form a linear chain at the upper level. The nodes are synched with the help of neighbor ID. The cluster head controls the various states of the node. Over The Air Programming (OTAP) network deployment is suggested to enable automatic software updation thereby reducing maintenance costs. The data collected from multiple sensors (acceleration, motion, temperature, infrared, vibration) in each node are aggregated and analyzed using a Decision Tree Classifier (J48). The classifier identifies the intrusion values from the normal values. The classification rate using J48 classifier was better than *ZeroR, DecisionTable, RandomForest and ADTree*. The authors claim that the continuous monitoring of the data collected at multiple sensors installed at each node results in a better prediction model.

An embedded anomaly detector was proposed by Raciti et. al [7]. An embedded anomaly detection model periodically collects both the cyber domain data (packet header, connections) and the physical data (energy measurements) and a feature vector is generated. BIRCH inspired incremental clustering algorithm [8] processes the feature vector based on the centroid distance threshold and the number of clusters to determine if it falls under a closest cluster. Several types of attack like data manipulation, recalibration, reset and sleep mode were detected with the algorithm.

In [9], PMU measurements from synchrophasors were analyzed by various classifiers like Naïve Bayes, OneR, NNge, JRipper, Random Forests and Adaboost and evaluated for Intrusion Detection Systems (IDS) to identify power System disturbances (both natural and malicious) in a smart grid. The classifiers were tested against three classification schemes based on the event occurrence: multiclass, three-class (attack/natural/no event) and binary (attack/natural). The performance evaluation showed that Random Forests, JRipper and Adaboost combined with JRipper exhibited high precision, OneR and Naïve Bayes exhibited average recall, JRipper and Adaboost combined with JRipper exhibited average recall and JRipper combined with Adaboost exhibited high F-measure. The overall performance evaluation indicated that JRipper combined with Adaboost, a coupling of a tree-based rule generation and a learning ensemble approach is the optimal classifier for a three-class classification scheme.

Ford et.al. [10] proposed an ANN based Intrusion Detection System (IDS) to predict the consumption behavior of the customer. The consumer's energy consumption behavior (ECB) profile included parameters like time and week in addition to the energy consumption data. This data is used to model the customer's consumption behavior using a neural network. The statistical analysis of the predicted value from the neural network compared with the real values helps to identify deviations.

Krishna et.al [11][12] [13] have extensively worked on anomaly detection with respect to meter frauds. In [11] ARIMA forecasting was evaluated and an integrated attack model was defined for detection anomalies in consumption data. In [13] a framework based on Kullback-Leibler Divergence (KLD) was proposed to detect the attack model. The authors have identified 5 classes of attacks and used the KLD to identify meter frauds such as multiple reading from the customer's tariff data. In [12], the authors proposed an anomaly detection based on Principal Component Analysis (PCA) to effectively monitor consumption readings.

The work in [13] is extended in [14] to evaluate signal processing-based detection approaches for meter frauds in alternate resources like solar and wind grid data.

In [15] Rossi et.al focused on detecting collective and contextual anomalies from a stream of smart meter event occurrences. In this paper, association rule mining is used to identify sets of recurrent events instances (frequent itemsets). The most frequent itemsets are extracted by applying an Apriori algorithm. These itemsets are augmented with contextual information. A categorical clustering based on entropy minimization to create clusters of similar categories of features. A clustering silhouette concept is used to identify the best fit of an itemset in an existing cluster. The authors were the first to propose the possibility of a collective and conceptual anomaly detection scheme.

Valdes et.al. [16] analyzed energy measurement samples to identify new data and similar patterns and by combining the concepts of adaptive resonance theory and self-organizing maps.In [17], both supervised and unsupervised machine learning techniques were used to identify stealth false data injection in a state estimation. PCA is used for dimensionality reduction and a distributed SVM is applied to distinguish a stealth attack from a normal attack. Ge.et.al [18] studied the performance of ANN on smart meter data such as line voltage and power load to detect load altering in the power grid. In [19], an Intrusion Detection System (IDS) was installed with sensors in all the network components (HAN, NAN and WAN). Data from the sensors in each of the network was preprocessed and tested on 20 classifiers. Five classifiers provided better precision: J48, JRip, BayesNet, SVM and MLP. J48 classifier showed the highest precision discovering all types of attack.

An IDS for the AMI architecture to protect data collected from devices like smart meter and AMI headend was proposed in [20] using CART decision tree because of its ability to perform both classification and regression. The network flow features are extracted from the traffic and decision tree is generated based on the CART algorithm.Chamie et.al [21] used the real time data from the μPMUs to identify transients caused by manipulating the electric devices (circuit breakers and switches). The proposed anomaly detection, Pseudo-Supervised Learning (PSL) algorithm is a two-step process that initially employs Isolation Forests, an unsupervised learning to capture the normal data features (termed as “pseudo label”) followed by non-linear regression, a supervised learning on the pseudo label to learn a model that best fits the features to the pseudo label. Thus, this approach can identify the anomaly features that are not part of a normal pattern.

Zhang et.al [22] proposed a semi-supervised Generative Gaussian mixture model (GMM) for analyzing the customer’s energy consumption data (from AMI infrastructure) to detect energy theft. The GMM model is used to generate the threshold from the customer’s previous consumption (non-malicious) data. The thresholds are compared with the new data to detect anomalous behaviours. An ensemble learning model that combines the results from multiple decision tress was proposed in [23] for a Transactive Energy Systems (TES). TES is an essential part of the smart grid that monitors the information transactions between various stakeholders in the grid to make decisions on energy consumption and demand response. The proposed ensemble approach combines the predictions called “confidence” from 10 decision tree models based on various controllers to generate a combiner measure called “plurality” to boost the overall performance.

Ayad et.al [24] investigated Recurrent Neural Networks (RNN) to detect False Data Injection (FDI) attacks in a smart grid. In RNN, the memory created with the information from previous outputs thereby storing sequential time information as state. This state information is used to predict the new state (output). The authors were the first to consider RNN as a tool for anomaly detection in smart grid. Schuster et.al. [25] proposed a self-learning network anomaly detection for a real-time energy network. The detector is trained with normal and anomalous traffic traces using six major classifiers.In [26], machine learning algorithms like Principal components analysis (PCA), Competitive Neural Network Learning (CNNL) and other statistical methods were used to analyze syslog data in a real-time smart grid to establish trust metrics between substations. Lore et.al. [27] proposed a server-centric anomaly detection framework that utilizes the correlation between spatial and temporal data from multi modal solar farms. The models were analyzed using Classification algorithms like vector autoregressive models (VAR), deep neural networks (DNN), long short-term memory networks (LSTM), inverse PCA reconstruction (iPCA) and deep auto-encoders (DAE) and evaluated for replay, correlation, delay, scaling and random attacks.

Ouyang et.al [28] extracted the time series features from power consumption data collected from IoT device in the grid. The extracted summary, transform and shift features are trained using multi-view learning model and stacking is applied. Pereira et.al [29] proposed a variational recurrent autoencoder and a variational selfattention mechanism (VSAM) based anomaly detection on time series data of a solar grid. Anomalous patterns are detected by using the probabilistic reconstruction metrics as anomaly scores.Yeckle et.al [30] explored the performance of seven outlier algorithms (Local Outlier Factor (LOF), Local Density Factor (LDF), Flexible Kernel Density Estimates (KDEOS), Influenced Outlierness (INFLO), Relative Density-based Outlier Score (RDOS), Mutual k-nearest neighbor (MNN) and Indegree Number (ODIN)) on AMI data preprocessed using k-means clustering achieving feature reduction. INFLO and RDOS outliers showed better performance. Veloso et.al [31] proposed the implementation of Cognitive Smart Plugs (SPs) for visualization and monitoring of residential area energy data using machine learning. The Electric Load Signature (ELS) generated from each SP (or SM) in a grid is filtered and identified using Decision Tree and Naïve Bayes learning algorithms.

Cui et.al [32] developed a machine learning anomaly detection methodology that combines k means clustering (unsupervised), Naïve Bayes (supervised) and dynamic programming to detect cyberattacks for load forecasting data. Buzau et.al [33] proposed the implementation of XGBoost Classifier on smart meter data such as EC, alarms and electrical magnitudes to detect the anomalies caused by non-technical losses such as installation error, meter parameterization error and faulty meter. Fenza et.al [34] proposed a context aware framework to detect anomalies in identifying energy consumption profiles (concept drift) by training a Long Short Term Memory (LSTM) model on profiles clustered using k-means clustering.In [35], an anomaly detection system based on feature grouping combined with linear correlation coefficient (FGLCC) algorithm is proposed where the ID3 classifier is used for decision making. Marino et.al [36] proposed a cyber-physical sensor (IREST) for detecting anomalies where unsupervised (One Class SVM) and supervised (Decision Trees and Random forests) learning models were used. In [37], Logistic Regression Analysis is implemented data from Synchrophasor systems, like Phasor Measurement Units (PMUs) for anomaly detection.

Roy [38] explored four classifiers: Random Forests, Naïve Bayes, XGBoost and SVM to implement network intrusion detection on highly unbalanced data. XGBoost and Random Forest showed better performance. Soleymani et.al [39] proposed unsupervised clustering-based approach and uses a correlation based stochastic method to locate the anomaly provenances that cause outage and energy theft. Trevizan et.al [40] proposed anomaly detection using Reed-Xaoli (RX) algorithm and a Chi-squared test for the detection FDI attacks in power system measurements.Deep learning techniques like deep auto-encoders were implemented in the distributed grid network [41] to address PMU data manipulation attacks. In [42] the unsupervised learning model was proposed based on GMM-LDA clustering for feature learning and PSO-SVM on smart meter data from AMI to trace abnormal power consumption. The integrated learning model performed better than the supervised SVM learning. Shafee et.al [43] proposes a deep recurrent neural network based anomaly detector learning model to detect Electric Vehicles (EVs) reporting false state of change values.in a smart grid. A Non-dominated Sorting Genetic Algorithm was used to perform an exhaustive grid search.

Sahu et.al [44] compared Logistic regression and artificial neural network (ANN) classification models on IoT networks and concluded ANN showed better precision. Shereen et.al [45] proposed two threshold-based and two machine detectors for monitoring time variables from the PMU clock system. The data-driven detectors were unsupervised Auto-Encoder Neural Network Detector and supervised Random Forest detector. However, the performance of threshold detectors was optimal compared to the machine learning detectors.
Ravikumar et.al [46] explored seven supervised learning models for classification and mitigation technique for anomaly detection in wide-area damping control (WADC). Barua et.al [47] proposed a neuro cognitive-inspired unsupervised learning model called Hierarchical Temporal Memory (HTM) to detect spatial and temporal anomalies in µPMU data. In [48], bidirectional RNN based anomaly detection was proposed for IEEE 1815.1-based network. The proposed system was effective for CPS malware behavior (CMB), false data injection (FDI), and disabling reassembly (DR) attacks.

Ma et.al [49] proposed a One Class SVM based anomaly detection to identify outliers in large scale energy data. In [50] One R, Random Forest, Naive Bayes and JRipper models were analyzed on a three class dataset for anomaly detection. Random Forest classifier exhibited highest detection rate. In [51], deep learning based anomaly detection and classification system were proposed by combining Autoencoder and Generative Adversarial Network (GAN). Ahmed et.al [52] proposed a distributer deep autoencoder based anomaly detection over PMU data streams.Khaledian et.al [53] combined three unsupervised classifiers for anomaly detection and classification on PMU time series data. The authors applied a kalman filter algorithm to condition the synchrophasor data.

4.1 Inferences from the Literature Survey:

The following points are inferred as a result of the above survey:

- Machine learning algorithms are highly utilized by anomaly detection systems because of the ability to acquire useful insights from historical data and make useful predictions. The outliers were able to mitigate most of the attacks caused in a smart grid.

- Machine learning algorithms approaches can be implemented on any type of framework to train and test the detection rate of the anomalies.
- The Advanced Metering Infrastructure (AMI) from the operations domain and Phasor Measurement Units (PMU) from the transmission domain are pivotal centers that generate grid data. Machine learning models are trained for data generated from both AMI and PMU.
- Deep learning models are ideal for the future smart grid anomaly detection systems as huge data with minimum human intervention can be monitored and trained.

5. Conclusion and Future Directions of Research

Smart grid infrastructure has the capacity to accommodate distributed energy resources to meet the rising energy crisis. However, the dynamic and bidirectional nature of the data in the grid makes anomalies inevitable incurring huge losses. Machine learning algorithms are progressive in the design of effective anomaly detection framework. In this paper, a chronological survey of the various machine learning approaches for anomaly detection in smart grids is presented. The survey reveals that multiple machine learning techniques are experimented against any proposed framework to analyze the anomaly detection rate. It is also seen that deep learning techniques are the future direction of research for the design of a secure smart grid.

References

[1] Z. Lu, X. Lu, W. Wang and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," 2010 - MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE, 2010, pp. 1830-1835, doi: 10.1109/MILCOM.2010.5679551.

[2] NIST (National Institute of Standards and Technology). 2010. Smart Grid Cyber Security Strategy and Requirements, The Smart Grid Interoperability Panel–Cyber Security Working Group, NISTIR 7628, August 2010.

[3] E. Pallotti and F. Mangiatordi, "Smart grid cyber security requirements," 2011 10th International Conference on Environment and Electrical Engineering, 2011, pp. 1-4, doi: 10.1109/EEEIC.2011.5874822.

[4] X. Fang, S. Misra, G. Xue and D. Yang, "Smart Grid — The New and Improved Power Grid: A Survey," in IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 944-980, Fourth Quarter 2012, doi: 10.1109/SURV.2011.101911.00087.

[5] S. Kher, V. Nutt, D. Dasgupta, H. Ali and P. Mixon, "A detection model for anomalies in smart grid with sensor network," 2012 Future of Instrumentation International Workshop (FIIW) Proceedings, 2012, pp. 1-4, doi: 10.1109/FIIW.2012.6378345.

[6] S. Kher, V. Nutt and D. Dasgupta, "Resilient hybrid overlay model for smart grid: RHM for smart grid," 2013 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), 2013, pp. 45-51, doi: 10.1109/CICYBS.2013.6597205.

[7] Raciti, Massimiliano & Nadjm-Tehrani, Simin, “Embedded Cyber-Physical Anomaly Detection in Smart Meters”, 2013 Conference: International Workshop on Critical Information Infrastructures Security, 2013, pp. 34-45, doi:10.1007/978-3-642-41485-5_4.

[8] Burbeck, Kalle & Nadjm-Tehrani, Simin, “Adaptive real-time anomaly detection with incremental clustering.”, 2007, Information Security Technical Report. 12. 56-67. 10.1016/j.istr.2007.02.004.

[9] R. C. Borges Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari and S. Pan, "Machine learning for power system disturbance and cyber-attack discrimination," 2014 7th International

Symposium on Resilient Control Systems (ISRCS), 2014, pp. 1-8, doi: 10.1109/ISRCS.2014.6900095.
[10] V. Ford, A. Siraj and W. Eberle, "Smart grid energy fraud detection using artificial neural networks," 2014 IEEE Symposium on Computational Intelligence Applications in Smart Grid (CIASG), 2014, pp. 1-6, doi: 10.1109/CIASG.2014.7011557.
[11] Badrinath Krishna, Varun & Iyer, Ravishankar & Sanders, William, "ARIMA-Based Modeling and Validation of Consumption Readings in Power Grids", 2016, 10th International Conference on Critical Information Infrastructures Security (CRITIS 2015) At: Berlin, Germany, pp: 199-210. doi: 10.1007/978-3-319-33331-1_16.
[12] Badrinath Krishna V., Weaver G.A., Sanders W.H. (2015) PCA-Based Method for Detecting Integrity Attacks on Advanced Metering Infrastructure. In: Campos J., Haverkort B. (eds) Quantitative Evaluation of Systems. QEST 2015. Lecture Notes in Computer Science, vol 9259. Springer, Cham. https://doi.org/10.1007/978-3-319-22264-6_5.
[13] V. B. Krishna, K. Lee, G. A. Weaver, R. K. Iyer and W. H. Sanders, "F-DETA: A Framework for Detecting Electricity Theft Attacks in Smart Grids," 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2016, pp. 407-418, doi: 10.1109/DSN.2016.44.
[14] V. B. Krishna, C. A. Gunter and W. H. Sanders, "Evaluating Detectors on Optimal Attack Vectors That Enable Electricity Theft and DER Fraud," in IEEE Journal of Selected Topics in Signal Processing, vol. 12, no. 4, pp. 790-805, Aug. 2018, doi: 10.1109/JSTSP.2018.2833749.
[15] B. Rossi, S. Chren, B. Buhnova and T. Pitner, "Anomaly detection in Smart Grid data: An experience report," 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2016, pp. 002313-002318, doi: 10.1109/SMC.2016.7844583.
[16] A. Valdes, R. Macwan and M. Backes, "Anomaly Detection in Electrical Substation Circuits via Unsupervised Machine Learning," 2016 IEEE 17th International Conference on Information Reuse and Integration (IRI), 2016, pp. 500-505, doi: 10.1109/IRI.2016.74.
[17] M. Ashrafuzzaman et al., "Detecting Stealthy False Data Injection Attacks in Power Grids Using Deep Learning," 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), 2018, pp. 219-225, doi: 10.1109/IWCMC.2018.8450487.
[18] Linqiang Ge, Wei Yu, Paul Moulema, Guobin Xu, David Griffith and Nada Golmie, "Detecting Data Integrity Attacks in Smart Grid", Book Chapter, Security and Privacy in Cyber-Physical Systems, O' Reilly, pp: 281-303, 2017.
[19] J. Shah, "Understanding and study of intrusion detection systems for various networks and domains," 2017 International Conference on Computer Communication and Informatics (ICCCI), 2017, pp. 1-6, doi: 10.1109/ICCCI.2017.8117726.
[20] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "An Anomaly-Based Intrusion Detection System for the Smart Grid Based on CART Decision Tree," 2018 Global Information Infrastructure and Networking Symposium (GIIS), 2018, pp. 1-5, doi: 10.1109/GIIS.2018.8635743.
[21] M. El Chamie, K. G. Lore, D. M. Shila and A. Surana, "Physics-Based Features for Anomaly Detection in Power Grids with Micro-PMUs," 2018 IEEE International Conference on Communications (ICC), 2018, pp. 1-7, doi: 10.1109/ICC.2018.8423024.
[22] Q. Zhang, M. Zhang, T. Chen, J. Fan, Z. Yang and G. Li, "Electricity Theft Detection Using Generative Models," 2018 IEEE 30th International Conference on Tools with Artificial Intelligence (ICTAI), 2018, pp. 270-274, doi: 10.1109/ICTAI.2018.00050.
[23] A. Arman, V. V. G. Krishnan, A. Srivastava, Y. Wu and S. Sindhu, "Cyber physical security analytics for transactive energy systems using ensemble machine learning," 2018 North American Power Symposium (NAPS), 2018, pp. 1-6, doi: 10.1109/NAPS.2018.8600639.
[24] A. Ayad, H. E. Z. Farag, A. Youssef and E. F. El-Saadany, "Detection of false data injection attacks in smart grids using Recurrent Neural Networks," 2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2018, pp. 1-5, doi: 10.1109/ISGT.2018.8403355.

[25] V. B. Krishna, C. A. Gunter and W. H. Sanders, "Evaluating Detectors on Optimal Attack Vectors That Enable Electricity Theft and DER Fraud," in IEEE Journal of Selected Topics in Signal Processing, vol. 12, no. 4, pp. 790-805, Aug. 2018, doi: 10.1109/JSTSP.2018.2833749.
[26] F. Schuster, A. Paul, F. M. Kopp and H. König, "Catching Intrusions: Classifier Performances for Detecting Network-specific Anomalies in Energy Systems," 2018 International Conference on Smart Energy Systems and Technologies (SEST), 2018, pp. 1-6, doi: 10.1109/SEST.2018.8495702.
[27] J. Obert, A. Chavez and J. Johnson, "Behavioral Based Trust Metrics and the Smart Grid," 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), 2018, pp. 1490-1493, doi: 10.1109/TrustCom/BigDataSE.2018.00209.
[28] K. G. Lore, D. M. Shila and L. Ren, "Detecting Data Integrity Attacks on Correlated Solar Farms Using Multi-Layer Data Driven Algorithm," 2018 IEEE Conference on Communications and Network Security (CNS), 2018, pp. 1-9, doi: 10.1109/CNS.2018.8433159.
[29] Z. Ouyang, X. Sun, J. Chen, D. Yue and T. Zhang, "Multi-View Stacking Ensemble for Power Consumption Anomaly Detection in the Context of Industrial Internet of Things," in IEEE Access, vol. 6, pp. 9623-9631, 2018, doi: 10.1109/ACCESS.2018.2805908.
[30] J. Pereira and M. Silveira, "Unsupervised Anomaly Detection in Energy Time Series Data Using Variational Recurrent Autoencoders with Attention," 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), 2018, pp. 1275-1282, doi: 10.1109/ICMLA.2018.00207.
[31] A. F. da S. Veloso, R. G. de Oliveira, A. A. Rodrigues, R. A. L. Rabelo and J. J. P. C. Rodrigues, "Cognitive Smart Plugs for Signature Identification of Residential Home Appliance Load using Machine Learning: From Theory to Practice," 2019 IEEE International Conference on Communications Workshops (ICC Workshops), 2019, pp. 1-6, doi: 10.1109/ICCW.2019.8756885.
[32] M. Cui, J. Wang and M. Yue, "Machine Learning-Based Anomaly Detection for Load Forecasting Under Cyberattacks," in IEEE Transactions on Smart Grid, vol. 10, no. 5, pp. 5724-5734, Sept. 2019, doi: 10.1109/TSG.2018.2890809.
[33] M. M. Buzau, J. Tejedor-Aguilera, P. Cruz-Romero and A. Gómez-Expósito, "Detection of Non-Technical Losses Using Smart Meter Data and Supervised Learning," in IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 2661-2670, May 2019, doi: 10.1109/TSG.2018.2807925.
[34] G. Fenza, M. Gallo and V. Loia, "Drift-Aware Methodology for Anomaly Detection in Smart Grid," in IEEE Access, vol. 7, pp. 9645-9657, 2019, doi: 10.1109/ACCESS.2019.2891315.
[35] S. Geris and H. Karimipour, "Joint State Estimation and Cyber-Attack Detection Based on Feature Grouping," 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), 2019, pp. 26-30, doi: 10.1109/SEGE.2019.8859926.
[36] D. L. Marino et al., "Cyber and Physical Anomaly Detection in Smart-Grids," 2019 Resilience Week (RWS), 2019, pp. 187-193, doi: 10.1109/RWS47064.2019.8972003.
[37] S. S. Noureen, S. B. Bayne, E. Shaffer, D. Porschet and M. Berman, "Anomaly Detection in Cyber-Physical System using Logistic Regression Analysis," 2019 IEEE Texas Power and Energy Conference (TPEC), 2019, pp. 1-6, doi: 10.1109/TPEC.2019.8662186.
[38] D. D. Roy and D. Shin, "Network Intrusion Detection in Smart Grids for Imbalanced Attack Types Using Machine Learning Models," 2019 International Conference on Information and Communication Technology Convergence (ICTC), 2019, pp. 576-581, doi: 10.1109/ICTC46691.2019.8939744.
[39] M. Soleymani and A. Safdarian, "Unsupervised Learning for Distribution Grid Line Outage and Electricity Theft Identification," 2019 Smart Grid Conference (SGC), 2019, pp. 1-5, doi: 10.1109/SGC49328.2019.9056579.

[40] R. D. Trevizan et al., "Data-driven Physics-based Solution for False Data Injection Diagnosis in Smart Grids," 2019 IEEE Power & Energy Society General Meeting (PESGM), 2019, pp. 1-5, doi: 10.1109/PESGM40551.2019.8974027.
[41] J. Wang, D. Shi, Y. Li, J. Chen, H. Ding and X. Duan, "Distributed Framework for Detecting PMU Data Manipulation Attacks with Deep Autoencoders," in IEEE Transactions on Smart Grid, vol. 10, no. 4, pp. 4401-4410, July 2019, doi: 10.1109/TSG.2018.2859339.
[42] L. Zhang, L. Wan, Y. Xiao, S. Li and C. Zhu, "Anomaly Detection method of Smart Meters data based on GMM-LDA clustering feature Learning and PSO Support Vector Machine," 2019 IEEE Sustainable Power and Energy Conference (iSPEC), 2019, pp. 2407-2412, doi: 10.1109/iSPEC48194.2019.8974989.
[43] A. A. Shafee, M. M. Fouda, M. M. E. A. Mahmoud, A. J. Aljohani, W. Alasmary and F. Amsaad, "Detection of Lying Electrical Vehicles in Charging Coordination Using Deep Learning," in IEEE Access, vol. 8, pp. 179400-179414, 2020, doi: 10.1109/ACCESS.2020.3028097.
[44] N. K. Sahu and I. Mukherjee, "Machine Learning based anomaly detection for IoT Network: (Anomaly detection in IoT Network)," 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI) (48184), 2020, pp. 787-794, doi: 10.1109/ICOEI48184.2020.9142921.
[45] E. Shereen and G. Dán, "Model-Based and Data-Driven Detectors for Time Synchronization Attacks Against PMUs," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 1, pp. 169-179, Jan. 2020, doi: 10.1109/JSAC.2019.2952017.
[46] R. Gelli and G. Manimaran, "Anomaly Detection and Mitigation for Wide-Area Damping Control using Machine Learning," 2020 IEEE Power & Energy Society General Meeting (PESGM), 2020, pp. 1-1, doi: 10.1109/PESGM41954.2020.9281615.
[47] A. Barua, D. Muthirayan, P. P. Khargonekar and M. A. Al Faruque, "Hierarchical Temporal Memory Based Machine Learning for Real-Time, Unsupervised Anomaly Detection in Smart Grid: WiP Abstract," 2020 ACM/IEEE 11th International Conference on Cyber-Physical Systems (ICCPS), 2020, pp. 188-189, doi: 10.1109/ICCPS48487.2020.00027.
[48] S. Kwon, H. Yoo and T. Shon, "IEEE 1815.1-Based Power System Security with Bidirectional RNN-Based Network Anomalous Attack Detection for Cyber-Physical System," in IEEE Access, vol. 8, pp. 77572-77586, 2020, doi: 10.1109/ACCESS.2020.2989770.
[49] B. Ma et al., "Positive Active Power Outlier Detection based on One-Class SVM," 2020 12th IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), 2020, pp. 1-4, doi: 10.1109/APPEEC48164.2020.9220568.
[50] M. Panthi, "Anomaly Detection in Smart Grids using Machine Learning Techniques," 2020 First International Conference on Power, Control and Computing Technologies (ICPC2T), 2020, pp. 220-222, doi: 10.1109/ICPC2T48082.2020.9071434.
[51] I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras and P. Sarigiannidis, "A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1137-1151, June 2021, doi: 10.1109/TNSM.2021.3078381.
[52] A. Ahmed, K. S. Sajan, A. Srivastava and Y. Wu, "Anomaly Detection, Localization and Classification Using Drifting Synchrophasor Data Streams," in IEEE Transactions on Smart Grid, vol. 12, no. 4, pp. 3570-3580, July 2021, doi: 10.1109/TSG.2021.3054375.
[53] E. Khaledian, S. Pandey, P. Kundu and A. K. Srivastava, "Real-Time Synchrophasor Data Anomaly Detection and Classification Using Isolation Forest, KMeans, and LoOP," in IEEE Transactions on Smart Grid, vol. 12, no. 3, pp. 2378-2388, May 2021, doi: 10.1109/TSG.2020.3046602.