A Short Review; Cyber Attacks And Detection Methods Based On Machine Learning And Deep Learning Approaches In Smart Grid

Received: 1 January 2023; Accepted: 6 March 2023 *Review Article*

Mehmet Karayel
Computer Engineering
Kocaeli University
Kocaeli, Türkiye
226112004@kocaeli.edu.tr

Nevcihan Duru
Faculty of Engineering and Natural Sciences
Kocaeli Health and Technology University
Kocaeli, Türkiye
nevcihan.duru@kocaelisaglik.edu.tr

Mehmet Kara
Faculty of Engineering and Natural Sciences
Kocaeli Health and Technology University
Kocaeli, Türkiye
0000-0001-7312-0503

***Abstract*—Power systems and smart grids constitute critical instruments of national security and the economy. In case of the power system malfunctioning, millions of people are affected. Furthermore, there are extreme financial losses, irreversible data casualties and service outages. Recently, the use of commercial smart measuring and control devices in the field of electricity and power systems has become widespread due to the development of applicable technologies and the reduction of the costs of devices. Although this situation has increased traceability and manageability, it also made smart grids more vulnerable to cyber threats compared to the traditional power systems used before. Cyber threats in smart grids are generally categorized as eavesdropping the data to possess detailed information about the system, tampering with data to disturb the system's stability, denial of services to block accessibility and injecting malicious software that can cause damage to the system. FDI attack is considered one of the most severe cyber-attack types due to its stealthy. FDI attacks disrupt the entire stabilization of the smart grid gradually. Machine learning and deep learning methods in supervised, semi-supervised and unsupervised domains have been widely used to protect smart grids against cyber threats by assisting conventional bad data detection mechanisms. Successful results have mainly been obtained by deep learning algorithms such as CNN and RNN. These algorithms have been supported with improved feature selection techniques to increase the accuracy of the detection and decrease the computational burden of the models. The purpose of the paper is to briefly summarize and combine the significance of smart grids, vulnerabilities of smart grids, cyber threats to smart grids, deep learning and machine learning methods applied against cyber-attacks, especially FDI attacks considered to be the most dangerous attack type and potential future research areas.**

Keywords—Power Systems, Smart Grids, Cyber Attack, False Data Injection Attack, FDIA, Machine Learning, Deep Learning, CNN, RNN, LSTM.

I. INTRODUCTION

As a result of the introduction of Industry 4.0 [1] and Industry 5.0 [2] with the development of technology, human-machine interactions have started to appear more in every field than ever before since 2010. In addition to the favorable benefits brought by these technologies, the energy demand has increased dramatically. At the same time, energy continuity and supply-demand balance are critical parameters that all countries and companies must monitor because a failure or any problem in these systems affects all infrastructure. Therefore, energy generation and distribution systems are at the forefront of critical infrastructures.

Considering that the resources are not infinite, energy demand triggers the finding of solutions for using the energy more efficiently in a controlled environment at an optimum level. At this point, smart grids that meet energy demands intelligently come into play with new features and capabilities compared to traditional electricity grids in terms of traceability and manageability.

Power systems and smart grids are becoming critical infrastructures in recent years. The dependency on the power system and smart grid is increasing rapidly. Many people are affected by any problem in the power system or smart grid, and the losses are very high in the cost and information domain. It is considered that smart grids are still vulnerable to cyber-attacks since they are an extension of legacy systems, supported by commercial devices with no advanced security infrastructure and a lack of security protocols already existing in other networks like the internet.

The rest of the paper is organized as follows: Section 2 presents the grid conceptual model and architecture including vulnerabilities and cyber-attack types to smart grids. Detection Methods of FDI attacks are detailed based on machine learning and deep learning algorithms in section 3. Finally, conclusions and potential research areas are supported in section 4.

II. SMART GRIDS AND CYBER ATTACKS

Smart grids are sophisticated systems of legacy grids with improved properties. They combine different types of electricity production (Distributed Energy Resources-DER), like solar power, wind power, hydroelectric, etc., in one framework. Smart grids comprise all processes from production to consumption of electricity. Smart grids have been made intelligent by Information and Communication Technologies (ICT) such as control panels, sensors, actuators, measuring devices and smart meters. The most important feature that distinguishes smart grids from traditional systems is that instead of transmitting electricity in one-way, communication and power flows are conducted in two-way.

Smart grids have transformed into highly complex structures due to integrated information and communication systems. To minimize the complexity and clarify standards, a conceptual model was initially proposed in 2010 [3]. The conceptual model has been revised periodically based on

recent developments. The up-to-date conceptual model [4] is depicted in Figure 1. In general, a smart grid consists of 7 main domains. Data and power flow are carried out between the Generation, Transmission, Distribution and Consumption domains. On the other hand, data transmission is conducted between Operation, Service Provision and Market domains.

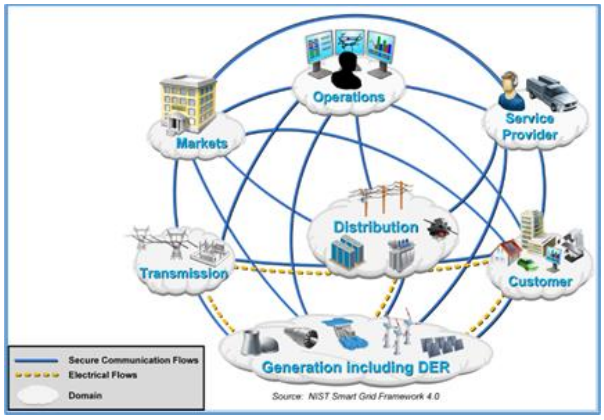

Fig. 1. The up-to-date NIST Smart Grid Conceptual Model.

A. *Security Vulnerabilities of Smart Grids*

Smart Grids uses Information and Communication Technologies (ICT) infrastructure to manage and monitor the system. ICT systems are vulnerable to cyber-attacks such as False Data Injections (FDI), Denial of Service (DoS), data sniffing, unauthorized access and password cracking. Smart grids are the target of ICS attacks as well as attacks against information systems. Therefore, the attack space is wider than the applied only in IT systems.

ICS systems are very different from Information systems in terms of performance, availability (reliability), risk management, system operation, resource constraints, communications, change management, support and component locations. As it can be understood from this structure, it is more challenging to control ICS system vulnerabilities compared to IT Systems only [5]. Vulnerabilities of smart grids can be grouped under the following main headings.

1) Physical Components Vulnerabilities: Hardware, software, and management systems make up a smart grid. However, they each have some vulnerabilities, such as insufficient physical access control, redundancy, component maintenance, and HAVC (Heating, Ventilation, and Air Conditioning) systems [6].

2) IT Vulnerabilities: One of the main functions of IT systems is automating business functions like billing, customer service, and accounting. Since the commence of the internet, IT systems have been employed, and a wealth of knowledge has been gained about them. There are many vulnerabilities, such as insecure software and hardware, confidentiality issues, integrity troubles and authentication and authorization problems. On the other hand, many critical areas, such as e-government, e-banking and e-commerce systems, are operated securely [7].

3) OT Vulnerabilities: A major focus of OT has been the management of power system operations, such as distribution of power and critical energy infrastructure management. OT advancements have led to more automated substations that can operate without human interaction. Software vulnerabilities in measurement devices, such as HMI (Human Machine Interface), RTU (Remote Terminal Unit), sensors and actuators, should be considered significantly critical matters which can lead to destructive cyber-attacks [8,9].

4) Data Processing and Management Vulnerabilities: Current smart grid data management faces the problem of data aggregation quality, security, compliance control, typical scope, and efficiency of the management mechanism. Many data are generated, processed, stored and transferred between different entities. The Confidentiality, Integrity and Availability of this data must be the focal points and be protected strictly. Data security and privacy should always be the priority in the design of smart grids [10].

5) Service and Application Vulnerabilities: The instant conversion of physical data into useful information is made possible by access to OT and IT data, enabling enhanced asset management platforms, distributed energy management systems, and distribution grid applications. Electricity trading, electricity services, electricity convergence, and a variety of client services are just a few of the applications and services that smart grids can offer. These services may include patching, policy, asset management, configuration, authentication, authorization, accounting and malware vulnerabilities.

6) Operational Environment Vulnerabilities: Unknowing employees, poor outsourcing, insecure configuration, and issues with the natural environment are some of the common risks for the operating environment of the grid.

B. *Cyber Attacks to Smart Grid*

Since 2010, there have been many examples that ended with financial losses and physical damage around the world. The most effective of all, attacks targeting Iran's nuclear facilities and Ukrainian power systems come to the fore. STUXNET targeted SCADA (Supervisory Control and Data Acquisition) systems and caused substantial damage to Iran's nuclear program, including the nuclear centrifuge, computers and ICS devices [11]. In 2016, a power system outage in Ukraine affected many part of the country and many customers [12].

Smart grid attacks are seen in a wide range, such as FDI attacks, denial of service (DoS) attacks, data framing attacks, man-in-the-middle attack, load altering attacks, false command injection attacks, load redistribution attacks, coordinated cyber–physical topology (CCPT) attacks and replay attack. These attacks can be grouped as IT-based, ICS-based and grid data based attacks. There are deep knowledge and preventive tools for IT-based attacks. Relatively less knowledge and preventive tools on ICS-based attacks and smart grid data based attacks.

As stated in the previous subsection, many critical areas, such as e-government, e-banking and e-commerce systems, can be operated safely in today's conditions where cyber-attacks are assumed and accepted. The infrastructure can be easily changed and adapted to new situations using simple costs in the mentioned areas. However, the situation is different in power systems and smart grids. As mentioned, power systems are being made smart by integrating commercial sensors and measurement systems of existing legacy systems. Therefore, advanced secure communication protocols and defense systems used on the internet are not used in power systems and smart grids. Artificial intelligence methods are included in the game precisely at this point.

Artificial intelligence fills the gap in the need for advanced security systems in smart grids.

FDI attack is considered one of the most severe cyber-attack types among the cyber-attacks mentioned above due to its stealthy. FDI attacks in a smart grid first appeared in [13]. They disrupt the entire stabilization of the smart grid gradually. Recently, FDI attacks received noticeable attention due to their impact. State estimation plays a critical role in the stable operation of smart grids at an optimum level. FDI attacks directly target state estimation. Failure to perform the state estimation process properly causes enormous damage and power outages. Because FDI attacks can be made relatively easily, but their damage to smart grids can be comprehensive, the methods applied against cyber-attacks are explained based on FDI attacks in the following sections.

III. Detection Of Cyber Attacks Using Machine Learning And Deep Learning Approaches

In the literature, studies were firstly based on simple and effective machine learning methods like Decision trees, Random Forests, etc., due to their simplicity and computational efficiency. After the deep learning methods became popular in other domains like image recognition and classification, deep learning practices such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN) and LSTM (Long-Short Term Memory) techniques were also widely applied for the detection of cyber-attacks in smart grids. Semi-supervised and unsupervised learning approaches are popularly used in this field, as accurate data on cyber-attacks in smart grids are rare and labelling datasets is highly time-consuming. Generally, in semi-supervised learning, unlabeled data is assigned to the nearest neighbor data set based on the labeled classes by kernel methods such as RBF (Radial Basis Function) or KNN (K Nearest Neighbor) [14]. In addition, to obtain more realistic training examples, a more advanced and complex model named Generative Adversarial Neural Network (GAN) is started to be used recently [15]. In the GAN model, labeled data are produced by two separate but linked Neural Networks, a generator and a discriminator, with feedback in an iterative min-max game.

Unlike supervised and unsupervised learning methods, fully unlabeled data is used to train the model in unsupervised approaches. Unsupervised methods such as Principal Component Analysis (PCA) and KNN-based methods are primarily and widely used in the literature [16].

Furthermore, the approaches to detecting cyber-attacks are categorized according to whether they depend on a model [17]. State estimation techniques in model-dependent and comparison of sequential temporal data in model-independent approaches are used based on the data collected during the system's regular operation. FDI attacks are targeted at the measurement data via tampering with the measurements to deceive the system. Traditional Bad Data Detectors can only be adapted for outlier information like false reading and cannot perceive hidden interventions like FDI attacks.

The most commonly applied Machine Learning and Deep Learning algorithms used to detect cyber-attacks in smart grids are summarized in Table I. Furthermore, the main strengths and weaknesses of the algorithms are indicated in terms of reinforcing knowledge about algorithms in Table II.

The strengths and weaknesses of the algorithms are assessed within the framework of general performance criteria. The assessments are made in terms of the internal structure of data, the data preprocessing phase, applying methods of algorithms, interior design and objectives of the algorithms, the algorithms' parameters, the algorithms' performance, the training phase of the algorithm, etc. In addition, only the most prominent features are highlighted in Table II.

TABLE I. Most commonly applied Machine Learning and Deep Learning algorithms

Learning Types	List of Algorithms
Machine Learning Algorithms	SVM (Support Vector Machine), KNN (K-Nearest Neighbor), ENN (Extended Nearest Neighbor), PCA (Principal Component Analysis), AdaBoost, Decision Tree, Random Forest, LGBM (Light Gradient Boosting Machine) and Logistic Regression.
Deep Learning Algorithms	ANN (Artificial Neural Networks), CNN (Convolutional Neural Networks), RNN (Recurrent Neural Networks), LSTM (Long-Short Term Memory) and GAN (Generative Adversarial Neural Networks).

TABLE II. Main strengths and weaknesses of the algorithms

Algorithm	Strengths	Weaknesses
SVM	1. Satisfactory performance in high dimensional space. 2. Outliers have a minor impact.	Slow training process for large datasets.
KNN	1. Simple to implement. 2. No presumptions about data.	Sensitive to outliers.
ENN	It can learn from the global distribution in addition to local one used in KNN.	Choosing of parameter “K” like KNN.
PCA	It reduces overfitting.	There is a possibility of information loss.
AdaBoost	It can be slightly less sensitive to overfitting.	It is susceptible to noisy data and outliers.
Decision Tree	Normalization or scaling of data not needed.	Prone to overfitting.
Random Forest	Promising performance on unbalanced and missing data.	It requires much computational power and time.
LGBM	Reduced training time and low memory usage.	It needs much complex trees.
Logistic Regression	Tuning of hyperparameters is not needed.	Inadequate performance on nonlinear data.
ANN	Suitable for modelling nonlinear data with a higher dimension.	There is no exact rule for defining the structure of the network.
CNN	It detects critical features in an unsupervised manner.	Training process may take considerable time depending on the number of network layers.
RNN	It is the first neural network able to analyse and learn sequences of data (series) of its kind.	Vanishing gradients.
LSTM	LSTMs are forceful RNNs designed to work with vanished gradients.	The training data required by LSTMs is much greater than that needed by CNNs and RNNs to achieve the same level of accuracy.
GAN	It can generate data similar to the original in an unsupervised manner.	Having two separate networks, a generator and a discriminator, makes training phase difficult.

It is evaluated that it would be helpful to explain the concept of "State Estimation" and "Bad Data Detector" approaches, which constitute the main pillars of controlling

and protecting the smart grids, are in the stage before the detection algorithms are applied. It also explains how FDI attacks are theoretically produced and why the BDD cannot recognize them.

A. State Estimation, Bad Data Detection (BDD) and False Data Injection Attacks

The main goal of state estimation is to predict a smart grid's current state using sensors' data. The measurements usually consist of real and reactive power injections of transmission lines and buses and state variables like all buses' voltage magnitudes and phase angles. In the state estimation, the relationship is conducted based on (1) between the state vector $x \in \mathbb{R}^D$ and measurements $z \in \mathbb{R}^N$. In addition, $H \in \mathbb{R}^{NxD}$ is Jacobian topological matrix and **e** is the error.

$$z = Hx + \mathrm{e} \tag{1}$$

The state of the smart grid can be predicted by Weighted Least Square (WLS) where W is a diagonal matrix with elements proportional to the variance of each measurement noise, defined as follows :

$$\hat{x} = arg_x\, min(z - Hx)^T W(z - Hx) \tag{2}$$

To eliminate the measurement error and sensor faults, BDD is applied as a first defensive mechanism to protect the state estimation. In the traditional BDD, the L2-norm of measurement residual is compared to the threshold τ and measurement data is not accepted when $\|z - \mathrm{H}\hat{x}\| > \tau$.

FDI attacks are created by adding an attack vector a to the measurement vector z. So state variable vector is transformed into (4) where $c \in \mathbb{R}^N$ is the difference in the state variable estimates. When the attack vector content with (5), then the L2 norm of attacked measurement is defined in (6). Equation 6 shows that L2 norm of attacked measurement residual does not change. It means that attacked measurements can bypass the BDD.

$$z_a = z + \mathrm{a} \tag{3}$$

$$\hat{x}_a = \hat{x} + \mathrm{c} \tag{4}$$

$$a = Hc \tag{5}$$

$$\|z_a - H\hat{x}_a\| = \|z + \mathrm{a} - \mathrm{H}(\hat{x} + \mathrm{c})\| \tag{6}$$

$$= \|z - \mathrm{H}\hat{x} + (\mathrm{a} - \mathrm{Hc})\|$$

$$= \|z - \mathrm{H}\hat{x}\|$$

B. Efficient Legacy Machine Learning Algorithms

The previous subsection explains the concepts of state estimation and BDD techniques, which indicate the current status of smart grids and lay the foundation for detection algorithms to be applied to detect cyber-attacks. This subsection details the recently applied machine learning methods for detecting cyber-attacks.

KNN algorithm, suitable for classification and regression purposes, is used as a main algorithm in [18, 19]. A Robust KNN regression approach is proposed in [18] to eliminate uncertainties and conduct more accurate state estimation in power systems. Furthermore, combining the KNN algorithm with PCA (Principal Component Analysis) feature selection based on the critical concept feature set is implemented in [19]. In addition to the studies in which KNN is the primary classifier, it is noteworthy that in other studies, it is usually in the domain of the compared algorithms. In [20], three common classifiers like SVM (Support Vector Machine), KNN and ENN (Extended Nearest Neighbor) algorithms were used for FDIA detection and SVM performed superior overall compared to KNN and ENN classifiers.

SVM, which avoids the difficulties of using linear functions in the high-dimensional feature space, is applied to detect cyber-attacks in smart grid that has a non-linear component in nature. In [21], an updated SVM-based method is proposed to detect the FDIA, bringing the vulnerabilities of existing SVM-based FDI attack detectors forward. Furthermore, a detection framework with an SVM classifier at its core with edge data aggregators to detect FDI attacks on transmission lines in [22].

Statistical models that prioritize catching the uncertainty in the models are used to detect the anomalies caused by FDI (False Data Injection) attacks. The multivariate Gaussian model improved with the k-means clustering method for detecting transient and steady cyber-attacks implemented in [23]. It is assumed that the multivariate Gaussian model captures the correlations between variables from different dimensions. In [24], a strategy based on statistical features is put forth to locate supervised FDI attacks in power grids. This method includes quantification of the distribution of the measurements and the tree boosting technique.

Random Forest algorithm, which can deal with both categorical and continuous variables efficiently, is also applied in this field. In [25], various classification methods, like Naive Bayes, Random Forest, etc., are used for detecting power system anomalies. The Random Forest algorithm gets the highest score among other methods. Furthermore, Isolation Forest Algorithm proposed with some acceptance criteria based on the Random Forest method in an unsupervised way in [26].

PCA technique which removes correlated features and reduces overfitting is commonly applied to improve the performance of models. In [27], high-dimensional space is reduced by KPCA (Kernel PCA) and the Extra-Trees algorithm is used to classify stealthy cyber-attacks. KPCA-supported Extra-Trees based detection approach outperforms the state-of-art machine learning-based schemes. Furthermore, [28] proposes a method for FDI attack detection based on PCA and subspace analysis utilizing consequential grid states.

Feature engineering aims to prepare an input dataset that best fits the machine learning algorithm and enhances the models' performance. Optimization algorithms and heuristic algorithms are commonly used. SVM is proposed as a primary classifier and compared to the other machine learning methods like AdaBoost and KNN to detect covert cyber deception assault attacks. Various feature selection methods including GA (Genetic Algorithm) are implemented. As a result, SVM has more successful results than other implemented algorithms [29]. In [30], SVM and KNN algorithms with three different feature selection methods, such as BCS (Binary Cuckoo Search), BPSO (Binary Particle Swarm Optimization) and GA (Genetic algorithm), are studied to detect the FDI attacks. SVM and KNN algorithms performed more

accurately compared to others. Furthermore, the AdaBoost classifier supported with Random Forest is used as the main of the proposed model with the enhanced feature construction engineering techniques in [31].

In [32], a framework combination of a square-root unscented Kalman filter (SR-UKF) based forecasting-aided State Estimation and a GLRT (Generalized Likelihood Ratio Test) is designed to detect FDI attacks in unbalanced distribution networks.

It is determined that SVM and KNN are applied much more than other machine learning algorithms to detect FDI attacks. Considering the complexity and non-linearity structure of the data obtained in smart grids, it has been observed that the SVM algorithm, built on the theory of creating a hyperplane, exhibits very reliable performances. Furthermore, the KNN algorithm is significantly utilized because it has a non-parametric and straightforward structure. In addition, KNN is ideal for non-linear data since there is no assumption about underlying data.

C. Deep Learning Algorithms

Convolutional Neural Network (CNN) is an artificial neural network architecture for deep learning with fully connected input, convolution, pooling and output layers that learn directly from data. Since the algorithm is based on learning directly from the data, invisible patterns can be revealed. Besides, RNN is a particular variant of ANN (Artificial Neural Network) for analyzing sequential data. Furthermore, the Long Short-Term Memory (LSTM) algorithm is an extension of RNN that extend the memory to eliminate the short-term memory. LSTM models can retain past information even longer compared to RNN algorithms.

Deep learning algorithms come to the fore in processing big data produced within the scope of monitoring and controlling smart grids to detect cyber-attacks. To facilitate big data processing, autoencoders within deep learning algorithms reduce the dimensionality of data and the computational complexity [33-35]. Furthermore, by using traditional machine learning algorithms and deep learning methods together, nonlinear data have been transformed into linear space and the detection accuracy of cyber-attacks has been increased [36].

Recently, deep learning algorithms combined with traditional machine learning algorithms such as SVM and KNN have been commonly used to detect cyber-attacks [37]. Furthermore, among the deep learning methods, LSTM, RNN and CNN are considered the most used and successful algorithms [38].

In [39], some ML-based models, such as SVM and Light Gradient Boosting Machine (LGBM) are compared with Deep Learning (DL) based models like CNN and ANN. As a result of the experiments, it has been determined that CNN models give better results. In [40], Continuous wavelet transform (CWT) is used to transform one-dimensional traffic data into a two-dimensional time-frequency domain as input to a wavelet CNN (WavCovNet) to distinguish the cyber-attack and detect abnormal behavior in the data.

Considering that smart grid data naturally contains linear and nonlinear components, an effective two-level FDIA detection is performed using the Kalman filter and RNN (KFRNN) [41]. In the first stage, the Kalman filter is used for state estimation from linear data and RNN is used to capture nonlinear data features. At the second level, the results obtained from the processes of linear and nonlinear are fed into a fully connected neural network with backpropagation. Furthermore, taking into account the same assumption accepted in [41] regarding linear and nonlinear components, RNN has also been proposed to detect the FDI attacks in [42].

Furthermore, [43] and [44] provide examples of how time series measurement values are effectively handled with RNN-based models. In [45], time domain data were processed with the LSTM autoencoder and anomalies are detected using the Logistic Regression. In [46], the state estimation to detect cyber-attacks is conducted through a model obtained by combining multiple LSTMs. In [47], the proposed framework is based on consolidating the Wasserstein Generative Adversarial Network and autoencoder to learn the smart grid measurement distribution and state estimator model.

As can be understood from the studies described above, deep learning algorithms such as CNN, RNN and LSTM and structures that combine these algorithms with traditional machine learning methods are widely and effectively used in detecting FDI attacks based on state estimation or time series. Furthermore, promising results have been obtained by using deep learning and machine learning algorithms together.

D. Simulations and Datasets

It would be helpful to specify the issue of obtaining the data. Since datasets regarding actual cyber-attacks are confidential and almost inaccessible, simulation methods are widely used to generate training and test data. The regular operation of the smart grid is simulated like a real-time environment to obtain the data. Furthermore, FDI attacks are implemented via tampering with the generated data.

In most of the studies, simulations are commonly conducted using the MATPOWER simulation package [48]. In addition, most of the simulations are performed based on IEEE Bus Systems Data. These systems consist of loads, capacitor banks, transmission lines and generators and their reference values.

E. Main Issues and Future Directions

Cyber-attacks against smart grids can be roughly grouped as obtaining individual or system data illegally, creating large-scale denial of services, and sabotaging the system using false data. Considering the characteristics of cyber-attacks and instances encountered in real life over the last 20 years, cyber-attacks can be exploited as destructive weapons.

Furthermore, cyber-attacks are highly concentrated in critical infrastructure areas such as energy generation, especially nuclear infrastructure, the nation's military and civilian defense systems, bank and finance systems, communication systems, logistic and critical commercial port systems and services.

In the last 20 years, the main issues that drive using of artificial intelligence solutions to defend smart grids are as follows:

- Power systems and intelligent grids become the most valuable resources of a nation,
- Confidentiality, integrity and availability of the information produced in power systems and smart grids is vital,

- The need for controlling and monitoring activities in power systems and smart grids,
- Easy access to the commercial measuring systems and control equipment and vulnerabilities of commercial devices,
- Limited resources and the need to use energy efficiently at the maximum level,
- Increasing self-operating activities in every field and the inevitability of automation in the Industrial 5.0 era,
- Most of the ICTs used in the energy generation area are dependent on obsolete technology, so unlike internet infrastructure,

The following items can serve as the basis for future studies and research to ensure power systems and smart grids have a higher level of security against various cyber-attacks and provide uninterrupted operation.

- Developing new frameworks for the detection of multiple cyber-attacks at the same time,
- A deeper understanding of determining fingerprints and features of cyber-attacks,
- Building up new cascaded frameworks applying more distributed controlling and detecting manners over the whole system,
- Creation of cyber-attacks more realistically with various deep learning algorithms in addition to the existing GAN algorithm to develop sound defense systems due to the rarity of real datasets related to the cyber-attacks.

IV. CONCLUSION

In this study, the structure and working principles of smart grids, the vulnerabilities of smart grids, the types of cyber-attacks against smart grids, the most harmful FDI attacks, the reasons behind why machine and deep learning algorithms are needed in smart grids, the idea of how detection algorithms are used to detect cyber-attacks, the simulation and datasets used in studies in this field are shortly reviewed.

It is observed that traditional machine learning and deep learning algorithms have been successfully applied alone in detecting cyber-attacks, and promising results have been obtained. In addition, it should be mentioned that machine learning and deep learning methods are used together, and satisfactory results are obtained. Furthermore, it has been determined that SVM and KNN out of machine learning algorithms and CNN, RNN and LSTM from deep learning are the most used methods in detecting cyber-attacks in the literature.

During the literature review, it was observed that detection models were generally developed against a single attack type. The development of models for detecting two different types of attacks by obtaining the similar feature set between attack types and conducting detections based on using this similarity can shed light on potential future studies.

REFERENCES

[1] S. Vaidya, P. Ambad, C. O'Fallon, S. Bhosle, "Industry 4.0 – A Glimpse," 2 nd International Conference on Materials Manufacturing and Design Engineering. 11-12 December 2017, Procedia Manufacturing 20 (2018) 1233-238, 2018.

[2] A.S. George and A.S.H. George, "Industrial Revolution 5.0: The Transformation of The Modern Manufacturing Process To Enable Man And Machine To Work Hand In Hand," Seybold Report. ISSN NO: 1533-9211. September 2020,

[3] GW. Arnold, DA. Wollman, GJ. FitzPatrick, D. Prochaska, DG. Holmberg, DH. Su, AR. Hefner, NT. Golmie, TL. Brewer, and M. Bello "2010 NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP, 1108, 2010.

[4] A. Gopstein, C. Nguyen, C. O'Fallon, N. Hastings, and D. Wollman, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0," NIST Special Publication 1108r4, 44(16), 3111-3123, 2021.

[5] K. Keith Stouffer and M. Pease, Guide to Operational Technology (OT) Security, NIST Publication, 2022.

[6] J. Xie, A. Stefanov, and C.C. Liu, Physical and Cybersecurity in a Smart Grid Environment. In Advances in Energy Systems: The Large-Scale Renewable Energy Integration Challenge, Wiley: Hoboken, NJ, USA, 2019, pp. 85–109.

[7] C.M. Mathas, C. Vassilakis, N. Kolokotronis, C.C. Zarakovitis, and M.A. Kourtis, On the Design of IoT Security: Analysis of Software Vulnerabilities for Smart Grids. Energies 2021, 14, 2818.

[8] Y. Xu, Y. Yang, T. Li, J. Ju, and Q. Wang, "Review on cyber vulnerabilities of communication protocols in industrial control system," in Proceedings of the 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, 26–28 November 2017.

[9] J. Lazaro, A. Astarloa, M. Rodríguez, U. Bidarte and J. Jimenez, A Survey on Vulnerabilities and Countermeasures in the Communications of the Smart Grid. Electronics, 10, 1881, 2021.

[10] M.Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," Comput. Network, vol. 169, 107094, 2020.

[11] S. Kriaa, M. Bouissou, and L. Pi`etre-Cambac´ed`es, "Modeling the stuxnet attack with bdmp: Towards more formal risk assessments," in 2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS), pages 1–8, 2012.

[12] R. Khan, P. Maynard, K. McLaughlin, D. Laverty, and S. Sezer. "Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid," 4th International Symposium for ICS & SCADA Cyber Security Research 2016 4, pages 53–63, 2016.

[13] Y. Liu, P. Ning, and M.K. Reiter, "False data injection attacks against state estimation in electric power grids," Proceedings of the 16th ACM Conference on Computer and Communications Security, CCS 2009, pp. 21–32. ACM, New York, NY, USA, 2009.

[14] S. Sharma, K. R. Niazi, K. Verma, and T. Rawat, "An efficient optimization approach for coordination of network reconfiguration and pv generation on performance improvement of distribution system," in Control Applications in Modern Power System. Springer, pp.269-278, 2021.

[15] Y. Zhang, J. Wang, and B. Chen. "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," IEEE Transactions on Smart Grid, 12(1):623–634, 2021.

[16] A. S. Musleh, M. Debouza, H. M. Khalid, and A. Al-Durra, "Detection of False Data Injection Attacks in Smart Grids: A Real-Time Principle Component Analysis," 45th *Annual Conference of the IEEE Industrial Electronics Society,* October 2019.

[17] F. Mohammadi, M. Saif, M. Ahmadi, and B. Shafai. "A Review of Cyber Resilient Smart Grid," 2022 World Automation Congress (WAC), Hybrid, San Antonio, TX, USA, October 11-15 2022.

[18] Yang Weng, Rohit Negi, Christos Faloutsos, and Marija D. Ili´c. Robust data-driven state estimation for smart grid. IEEE Transactions on Smart Grid, 8(4):1956–1967, 2017.

[19] M. Mohammadpourfard, Y. Weng, M. Pechenizkiy, M. Tajdinian, and B. Mohammadi-Ivatloo, "Ensuring cybersecurity of smart grid against data integrity attacks under concept drift", Int. J. Electr. Power Energy Syst., vol. 119, p. 105947, Jul. 2020.

[20] J. Yan, B. Tang, and H. He. "Detection of false data attacks in smart grid with supervised learning," 2016 International Joint Conference on Neural Networks (IJCNN), pages 1395–1402, 2016.

[21] B. Wang, P. Zhu, Y. Chen, P. Xun, and Z. Zhang, "False Data Injection Attack Based on Hyperplane Migration of Support Vector Machine in Transmission Network of the Smart Grid," Symmetry, Vol. 10(5), May 2018.

[22] P. Xun, P. Zhu, Z. Zhang, P. Cui, and Y. Xiong, "Detectors on Edge Nodes against False Data Injection on Transmission Lines of Smart Grid," *Electronics*, Vol. 7(6), Jun. 2018.

[23] Y. An and D. Liu, "Multivariate Gaussian-Based False Data Detection against Cyber-Attacks," IEEE Access, vol. 7, pp. 119804–119812, 2019.

[24] J. Jiang, J. Wu, C. Long, and S. Li, "Location of False Data Injection Attacks in Power System," *2019 Chinese Control Conference*, Jul. 2019.

[25] M. Panthi, "Anomaly detection in smart grids using machine learning techniques," 2020 First International Conference on Power, Control and Computing Technologies (ICPC2T), pages 220–222, 2020.

[26] S. Ahmed, Y. Lee, S. H. Hyun, and I. Koo, "Unsupervised Machine Learning-Based Detection of Covert Data Integrity Assault in Smart Grid Networks Utilizing Isolation Forest," IEEE Trans. Inf. Forensics Secur., vol. 14, no. 10, pp. 2765–2777, October 2019.

[27] M. R. Camana Acosta, S. Ahmed, C.E. Garcia, and I. Koo, "Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks," IEEE Access, vol. 8, pp. 19921–19933, 2020.

[28] E. Drayer and T. Routtenberg, "Intrusion Detection in Smart Grid Measurement Infrastructures Based on Principal Component Analysis," *2019 IEEE Milan PowerTech*, Jun. 2019.

[29] A. Saeed, L. Youngdoo, H. Seung-Ho, and I. Koo. "Feature selection–based detection of covert cyber deception assaults in smart grid communications networks using machine learning," IEEE Access, 6:27518–27529, 2018.

[30] J. Sakhnini, H. Karimipour and A. Dehghantanha, "Smart Grid Cyber Attacks Detection Using Supervised Learning and Heuristic Feature Selection," 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, pp. 108-112, 2019.

[31] D. Wang, X. Wang, Y. Zhang, and L. Jin, "Detection of power grid disturbances and cyber-attacks based on machine learning", J. Inf. Secur. Appl., vol. 46, pp. 42–52, Jun. 2019.

[32] S. Wei, J. Xu, Z. Wu, Q. Hu, and X. Yu, "A False Data Injection Attack Detection Strategy for Unbalanced Distribution Networks State Estimation," IEEE Transactions on Smart Grid, in press.

[33] S.H. Majidi, S. Hadayeghparast, and H. Karimipour, H. "FDI attack detection using extra trees algorithm and deep learning algorithm-autoencoder in smart grid," International Journal of Critical Infrastructure Protection, 2022.

[34] J. Ding, A. Qammar, Z. Zhang, and H. Ning, "Cyber Threats to Smart Grids:Review, Taxonomy, Potential Solution and Future Directions," MDPI, 2022.

[35] L. Gotsev, B. Jekov, Y., Parusheva, and E. Kovatcheva, "Cyber Threats on Smart Grid: Concerns, Attacks and Advanced Detection," 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), 2022.

[36] T. Teng and L. Ma, "Deep learning-based risk management of financial market in smart grid, " Computers and Electrical Engineering, 2022.

[37] D.M., Menon and N.A. Radhika, "Trust-Based Framework and Deep Learning-Based Attack Detection for Smart Grid Home Area Network.", International Journal of Intelligent Engineering and Systems, 2022.

[38] R. Rituraj, "An Investigation into Methods and Applications of Deep Learning in Smart Grid," ICCC 2022, 10th Jubilee International Conference on Computational Cybernetics and Cyber Medical Systems, 2022.

[39] A. Khan, "Detection of False Data Injection Cyber-Attack in Smart Grid by Convolutional Neural Network-Based Deep Learning Technique," Lecture Notes in Electrical Engineering, 2022.

[40] H.N. Monday, J.P. Li, G.U Nneji,. A.Z. Yutra, B.D. Lemessa, S. Nahar, E.C. James, and A.U. Haq, "The Capability of Wavelet Convolutional Neural Network for Detecting Cyber Attack of Distributed Denial of Service in Smart Grid," 18th International Computer Conference on Wavelet Active Media Technology and Information Processing, ICCWAMTIP 2021, 2021.

[41] Y.Wang, Z. Zhang, J. Ma, Q. Jin, "KFRNN: An Effective False Data Injection Attack Detection in Smart Grid Based on Kalman Filter and Recurrent Neural Network," IEEE Internet of Things Journal, 2022.

[42] Y. Wang, W. Shi, Q Jin, and J. Ma, "An accurate false data detection in smart grid based on residual recurrent neural network and adaptive threshold," IEEE International Conference on Energy Internet, ICEI 2019, 2019.

[43] Y. Wang, D. Chen, C. Zhang, X. Chen, B. Huang, and Cheng, X., "Wide and Recurrent Neural Networks for Detection of False Data Injection in Smart Grids," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019.

[44] 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 and Energy Society Innovative Smart Grid Technologies Conference, ISGT 2018, 2018.

[45] L. Yang, Y. Zhai, Z. Li, "Deep learning for online AC False Data Injection Attack detection in smart grids: An approach using LSTM-Autoencoder," Journal of Network and Computer Applications, 2021.

[46] M. Alazab, S. Khan, S.S.R. Krishnan, Q.V. Pham, M.P.K. Reddy, and T.R. Gadekallu, "A Multidirectional LSTM Model for Predicting the Stability of a Smart Grid," IEEE Access, 2020.

[47] N.C. Enriquez, and Y. Weng, "Attack Power System State Estimation by Implicitly Learning the Underlying Models, " IEEE Transactions On Smart Grid, VOL. 14, NO. 1, January 2023.

[48] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," IEEE Trans. Power Syst., vol. 26, no. 1, pp. 12–19, Feb. 2011.G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.