A Brief Survey on Anomaly Detection in Smart Grid

Sreeja Matturu[1], Satya Jayant Misra[2]

***Abstract*— Smart grid is a powerful distributed energy network that performs a two-way communication between the consumers and the utilities. This can be considered as a complex system that interconnects various physical components like power plants and logical components like communication protocols and infrastructure. The main theme of smart grid is to distribute the electricity efficiently and acquire the data about electricity usage and transmit it back to the control center with the help of sensors attached to it. While the communication is in progress, some kind of irregularities like physical system faults or data hacking happens and results in delivering the wrong data. These kinds of anomalous behavior must be detected, else it deliver the wrong information and leads to make a wrong decision that can affect the efficiency of power distribution. In this paper, a survey on different types of attacks that can happen within the smart grid and proposed latest defense strategies that can protect the system from these attacks are explained in detail.**

***Index Terms*— Smart Grid, Types of Attacks, Anomaly Detection Techniques.**

I. INTRODUCTION

In a smart grid, the term "grid" stands for an electric grid which connects different substations, transmission lines and transformers to transmit the power by using transmission lines and distribute the power across different consumer nodes with the help of distribution lines[1]. Traditional electric grid system is considered only as a one-way communication. When the smart grid came into existence, it made a two-way communication system such that, it performs a better way of communication between the utilities and the consumers in a smart way. The two-way system has a power transmission as one way and acquiring the data back with the help of sensors that are equipped in the transmission lines from the consumer is the two-way processing. The electricity is produced every less than a micro-second, and the sensors record the amount of electricity producing every microsecond.

In order to record the amount of electricity use, smart homes installing the smart meter devices that allow the consumer to know the amount of electricity they use every day. In addition to that, smart grid has a better advantage of utilizing renewable resources like solar power, wind turbines, etc. to generate power which is automatically redirected to the distribution lines. This idea saves the electricity that is produced by the natural resources like coal, nuclear, etc. This way, smart grid has better efficiency in generating the power and distributing them. There are other advantages of using the smart grid. For example, it has automated maintenance and power reliability. If a substation fails to transmit the power, it automatically connects to the other substations and transmit the electricity. Smart grid has a number of benefits for using them to have an efficient power distribution.

A. Architecture

Figure 1 shows the operation of a smart grid architecture. The main observation from this figure is that, every node is interconnected, and it performs a two-way communication with the other nodes. There are three nodes that has an upper hand in generating and transmitting the electricity: Power generation company, the transmission system operator and the distributed network operators. The job of the power generation company is to produce the power in bulk and transmit the power to the substation. Substation transmit the power to the distribution substation, where it reduces the power to the limit of each node. Finally, it transmits the power to the consumer nodes. In between, renewable resources like wind and solar power are utilized and redirected to the distribution station to manage the transmission of the power. During this process, the data is generated from each node and transmitted back to the control system operators. The control operators analyze the data about the electricity usage continuously.

B. Motivation

In smart grid, data is produced and transmitted less than every microsecond. In this process, the data will be communicated between different substations and control centers. During the communication process, if any kind of failure or fault happens, then it will generate the data with some irregularities. These kind of irregularities happens because of some accidental errors like failure of power system, transmission, distribution cable degradation, or some malicious attacks like injecting some false data to reduce or increase the amount of power consumption. These kind of anomalies produces false alarms in the control center. These types of anomalies will generate wrong data, and it leads to make wrong decisions about power generation.

C. Problem Statement

Ensuring reliability and security is an important aspect while dealing with the smart grid system. In the two-way communication process in the smart grid, any type of attack might occur and generates wrong information about the electricity usage. In this survey, the study is focused on different types of attacks that can happen in the smart grid system. During the research, two major attacks that disturbs the entire power system were observed. First, is the physical attacks that mainly happens because of some physical-related faults. And the second is the cyber-attacks, which mostly relates to cyber hacking like injecting false data into the

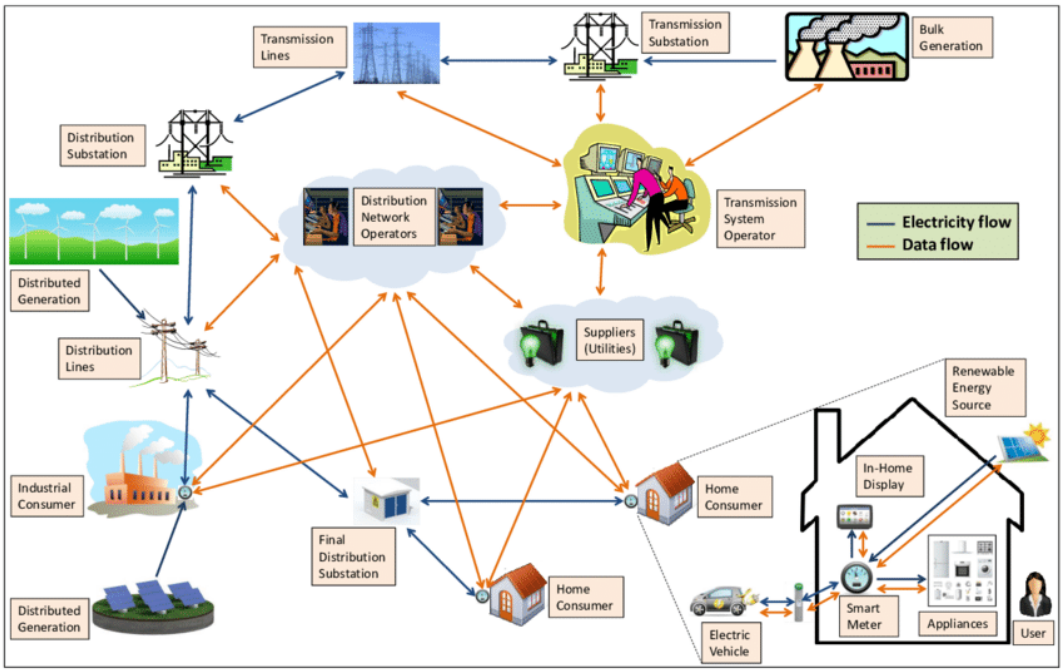

Fig. 1. Smart Grid Architecture[2]

system to either reduce or increase the amount of power consumption. Different sub attacks that come under these two attacks were studied and based on this, different anomaly detection techniques that can help to detect these attacks and safeguards the systems were discussed in detail.

This paper includes: (i) the related work about the previous anomaly detection techniques on different types of attacks are represented in Section 2, (ii) Section 3 that discusses about various security objectives. (iii) the detailed description of the problem about various kinds of physical and cyber-attacks are described in Section 4, (iv) Section 5 focuses on the different types of the latest anomaly detection techniques categorized for both physical and cyber-attacks and (v) Section 6 presents the overview of lessons learned during the research, which is followed by (vi) Section 7 conclusion and future directions.

II. Related Work

In this related work, the previous literature that was done in describing the attacks and proposed anomaly detection techniques in smart grid were presented. In paper [3], the main focus is made on smart grid infrastructure system and discussed about privacy and security issues in smart grid. The papers [4], [5] proposed about various types of security objectives and requirements and along with that, anomaly detection techniques which were proposed prior to these papers was discussed in detail.

In [6], Rough set theory and K-cross validation are proposed to analyze the condition of various protecting devices to secure the system without anomalies. In order to protect the privacy of the customers, a group-based anomaly detection[7] is implemented using bottom up approach that has lightweight based on kernel density estimator, which has the ability to localize the false data that has been inserted to detect the sudden events. In paper[8], a research analysis was made on the contextual anomaly detection method on a distributed grid that has low voltage. DER and power system analysis's are made to detect the abnormal behavior of the system with the best accuracy. In [9] an anomaly detection architecture was designed with the help of network security cyber sensor method to detect the cyber-attacks and improve the system security by allocating the sensitivity threshold value dynamically and used Interval Type 2 fuzzy logic system is implemented to describe the possibility of having a cyber-attack.

A prediction model as a hybrid sensor network was implemented in [10] as smart grid monitoring framework by using ZeroR, Decision Table, Random Forest, AD Tree and Decision Tree machine learning algorithms on the classification analysis. Results show that Decision Tree has the best classification rate of 97 percent. For analyzing and detecting the abnormal events, the authors of this paper[11] proposed a sparse approximation theorem, and an anomaly detection algorithm that uses wavelet projection to estimate the value and perform anomaly detection for the long-lasting behavior of the system.

A distributed anomaly detection based on deep learning techniques is implemented to detect high consumption of operation energy that has an IoT based distributed structure[12], which uses master-slave architecture and each slave has a stacked sparse encoder utilized for pulling out the high-level smart meter monitoring data automatically. Softmax was used to send the alarm messages to the IoT master node by using web technologies. This method gained good recog-

nition rate and best accuracy with reduced computational delay.

[13] discussed various types of malicious attacks and proposed a light-weighted pattern matching technique called as Graph Neuron for detecting the malicious attacks. In case of wide area monitoring, an anomalous behavior model which is based on spatial-temporal correlation[14] that has the ability to detect the anomalies like transmission line outages and a real time anomaly detection algorithm (ReTAD) is designed for handling the large amounts of data volume. The authors of [15] paper investigated on designing an optimal strategy for the flexible region for attacking a single line and thus avoids the need of heavy network information.

All the previous work was related to the detection techniques that were proposed about 8 to years 10 years ago. Other surveys were published in the year 2015 and 2016 describing all the previous techniques implemented. In this paper, the focus was made on a survey with different types of attacks and their anomaly detection techniques, which were implemented from 2016 to 2020.

III. Security Objectives

In smart grid, there are two types of data that can be exchanged between the utilities and the consumers. First one is the operational data, which means the amount of electricity that is produced and transmitted to the other nodes. Second one is the information data, which consists the information about the amount of electricity use at each node. During the communication process, there are specific objectives to ensure the security of the smart grid system. They are confidentiality, integrity, availability, authentication and authorization[5].

- Restricting the unauthorized users in trying to access the information which is confidential to protect the privacy and security to ensure the confidentiality of the smart grid infrastructure.
- Restricting the adversaries who attempts to modify the sensor data and produce wrong information which could lead to integrity loss is considered as protecting the integrity of the system.
- Accessing the data generated by the smart grid on time is the availability of the data. Loss of data can cause flooding attacks which leads to Denial-of-Service and Distributed DoS attacks.
- Authentication is validating the identity of the communication systems. If the authentication is lost, then the attacker has a great chance of gaining the access to the private information to use the smart grid system accordingly.
- Authorization is providing the access to the smart grid system to operate the device and provide proper management of the data and other resources.

IV. Types of Attacks

Figure 2 shows the various types of attacks that affect the smart grid infrastructure. As discussed in the previous section, two major attacks namely physical and cyber-attacks are explored. There are other types of attacks that comes under the physical and cyber-attacks that are described in detail below.

A. Physical Attacks

The word "physical" refers to some kind of physical components like the grid, cables, transformers, substations, distribution lines, etc. For example, when substations does not work or when distribution line fails in the smart grid, or sudden failures of physical components, then it is considered as a physical attack. Some of the physical attacks described in this study are power consumption attack, power fluctuations, operation energy consumption and electric faults.

1) Power Consumption Attack: This type of attack happens when suddenly the amount of power being consumed becomes very high or very low. During the transmission of the electricity continuously, there are some peak time intervals line evening hours where the consumption of power becomes very high and manage the amount of power to be generated and distributed efficiently. If not, it will raise an alarm for power consumption. This can happen due to cyber attack as well.

2) Power Fluctuations: Fluctuations are defined as the sudden on and off actions that especially happens when there is bad weather such that the cables, substations, and other physical components gets affected and disturbs the normal electricity flow to the other nodes. For example, when there are thunderstorms, then suddenly there will be a power outage and gets restored after sometime.

3) Operation Energy Consumption: Operation energy relates to the use of basic operations like light bulbs, ventilators, cooling systems, etc. Heavy usage of these operations can result in increasing the amount of energy consumption. If the operation energy consumption increases, then it also the increases the electricity bill[12].

4) Electric faults: These type of faults are referred as malfunctions of the physical entities such as degradation and abnormal performance. These type faults can happen like cable degradation, grid failures, etc. These components could generate wrong data and transmits high or low amount of power to the other nodes.

B. Cyber-Attacks

Cyber-attacks are the biggest threats for effecting the security smart grid that are mostly related to attack the data in the form of hacking the system or falsifying the data to affect the entire system. Cyber-attacks are classified into three types of attacks. First one is confidentiality target attack, second one is the integrity target attacks and the last one is the availability target attacks. Each of the attack is described detail in the following[16].

1) Confidentiality Target Attacks (CTA): The main theme of this attack[16] is to acquire the unauthorized access to the data which is confidential without disrupting the communication to affect the electricity markets. These types of attacks include privacy issues, eavesdropping, message replay attacks, etc.

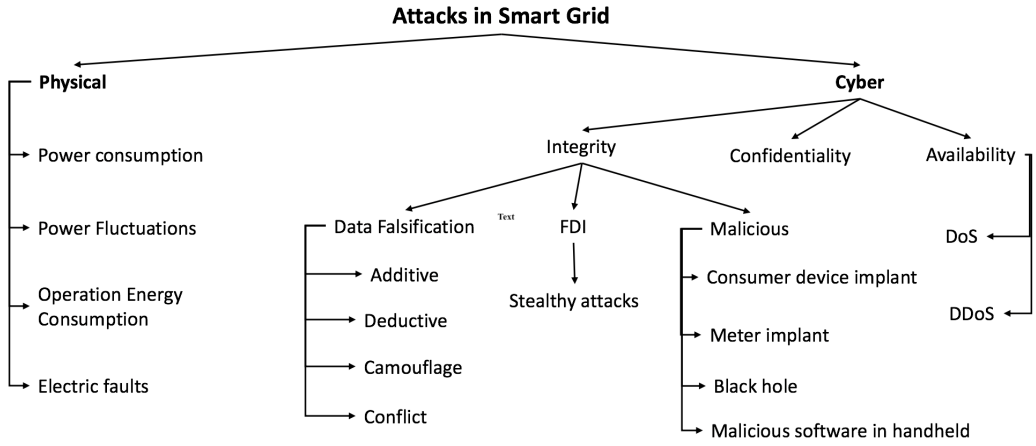

Fig. 2. Classification of Attacks in Smart Grid

2) Integrity Target Attacks (ITA): These attacks[16] are caused by the adversary attempts trying to inject wrong data into the system and generate false alarms. This type of attack also happens due to malicious software installation, compromising smart meters or falsifying the data of smart meters which creates data falsification attack, false data injection attack and the malicious attacks.

- Data Falsification Attacks: This type of attack[17] happen when the intruder tries to compromise the smart meter and report false amount power consumption either to increase or reduce the electricity bill. This kind of attack is called as "electricity theft".
  In addition to that, there are four data falsification strategies were discussed. First one is the additive attack, second one is the deductive attack, next one is the camouflage attack and the last one is the conflict attack.
  - Additive attacks are defined in a scenario when there are large number of tampered smart meter devices are installed and the adversaries trying to report high amount of power consumption than the genuine use of electricity.
  - With the same scenario, when the adversary tries to isolate the smart meters and reduce the amount of power consumption to reduce the electricity bill, then it is considered as a deductive attack.
  - Camouflage attacks are the balanced attacks of both additive and deductive attacks, which occurs in the same margin of data falsification type and produce low electricity bills for one set of consumers without raising any suspicious activity and lies undetected by avoiding to attack other components in the grid to escape from the consistency checks.
  - Conflict attacks are the unequal margin of an underlying simple attack type. When suddenly, many number of adversaries launches many number of attacks at the same instant, then all the attacks will get conflicted.
- False Data Injection Attacks: False data injection attacks are caused by the adversaries who tries to hack into the sensor data and inject wrong information about the electricity usage to raise false alarms. For example, if the voltage required for a node is 120kW and it is transmitted by the distribution line. When the adversary hacks into the data and modify the voltage to 500kW, then it will raise a false alarm saying that the amount of voltage is increased even though the grid is working fine. This can lead to either increase or decrease the amount of electricity bill.
  - Stealthy attacks are the secret attacks which makes impossible to detect with the help of traditional anomaly detection techniques.
- Malicious Attacks: The adversaries launching attacks to disrupt the daily operations of the smart grid infrastructure. Different types of malicious attacks are classified as follows [13]:
  - Consumer device implant attacks motive is to provide the data, which consists of falsified information about the electricity use to increase the electricity bills. If there is no secure communication between the meters and the devices, these attacks can cause grievances to the consumers and the smart grid administrators.
  - When a smart meter is installed with some malicious software so that, it can falsify the meter readings either to increase or reduce the electricity bill for a given consumer. The main motive behind this attacks is to disrupt the routine operations of the smart grid infrastructure system.
  - If some kind of communication process or data concentrator behaves abnormal all of a sudden due to some malicious software installation then, it can cause the black hole attacks which means the meter readings will not reach the destination and can cause disruption to the functionality of the smart grid infrastructure system.
  - When hand-held devices with internet connectivity

to record readings got compromised by some worm or virus and are used with the smart grid system, then the virus will be transmitted and effects the functionality of the smart grid system and cause consumer annoyances.

3) Availability Target Attacks (ATA): Due to continuous availability, a smart meter has a high chance of exposing towards attacks. There are two major attacks that targets the availability of the system. First one is the Denial-of-Service (DoS) attack where the system gets flooded with the continuous requests and thus makes a delay in providing the service known as flooding attack. Second one is the Distributed Denial-of-Service attack[18] as a malicious attempt, which mainly tries to disrupt the normal traffic of a targeted network by flooding with the internet traffic.

V. Proposed Anomaly Detection Techniques

Section IV described about various types of cyber attacks that occur within the smart grid infrastructure. In this section, different types of proposed anomaly detection techniques for the attacks that are classified in Figure 2 are explained in detail.

A. Physical Attacks

Table I represents the different types of physical attacks and their proposed anomaly detection technique references. Each of the proposed technique are described in the following.

TABLE I
Detection techniques of Physical Attacks

Physical Attack	References
Power Consumption Attack	[19]
Power Fluctuations	[20], [21], [22]
Abnormal Behavior	[23], [24], [25]
Electric Faults	[26], [27], [28]

The paper[19] detected the anomalous pattern attacks of power consumption attack by using wavelet transform, variance fractal dimension and artificial neural networks which allows to detect the anomalies fast, accurate and resistant to noise and sensitive to various kind of attacks. [20], [21] talks about power fluctuations and handles the huge amounts of data that is generated by PMU for communication and bandwidth by using single board computers so that it can provide local monitoring of efficient energy. [22] discusses about anomaly detection for power fluctuations with a two-step anomaly detection approach with MapReduce paradigm is proposed that mainly helps in leveraging the data fidelity and accuracy of the data. If any kind of alarm events occur during the algorithm, then it detects the anomalies with alarm events and communicated to the grid operator by using user interface.

A real time anomaly detection method is implemented to detect the anomalous events and the system abnormal conditions at both customer and lateral levels in [23]. The main theme behind implementing this framework is to combine all the smart meter data measurements under same lateral and include these measurements into the framework to produce perception at both customer and lateral levels. The main intention in [24] is to study on large anomaly detection on the data to detect abnormal behavior patterns by using frequent itemset mining and categorical clustering with a clustering silhouette threshold. Top 10 types of anomalies can be detected in the data based on the assigned threshold value.

The paper[25], emphasizes on the importance of context (which is valuable in determining accuracy) of domain in the smart grid and choosing the approach of detecting anomalous behavior such as heterogeneity and complexity of technology. They classify most of the literature technique as data mining technique and machine learning technique in their effectiveness context base anomaly detection.

Paper[26] used power line modems as network sensors for the sake of wide bandwidth to detect the electric faults. Symbol level sensing and main level sensing are used for monitoring the data. Paper[27] proposed LSTM abbreviated as long short-term memory technique, which is a type of recurrent neural network has the ability to predict the behavior of the consumer based on the past consumption's and this method is known as concept drift. The paper[28] presented a probabilistic reconstruction score to detect anomalous behavior in solar energy by using variational self-attention mechanism (VSAM) to improve the encode and decode procedure.

B. Cyber-Attacks

In this section, different types of new anomaly detection techniques are described for detecting the various cyber threats. Table II gives an overview about types of cyber attacks and their implemented techniques references. List of implemented techniques are explained in detail in the following.

TABLE II
Detection Techniques of Cyber Attacks

Cyber Attack	References
Confidentiality Target Attack	[29], [30]
Integrity Target Attack	[31], [32]
False Data Injection	[33], [34], [35], [36], [37], [16], [38]
Data Falsification	[17], [39]
Denial-of-Service	[40], [41], [42]
Distributed Denial-of-Service	[43]

In paper[44], an outlier detection model named Clustream that is defined as a streaming clustering approach was implemented for detecting the anomalous users and compared with DBSCAN algorithm. In case of missing data or some error data is recorded, then a data pre-processing method is used to detect the errors or missing data while smart grid is acquiring the data. The two-phase proposed method achieved the detection rate of 98 percent and does detected the anomalous users in streaming power data.

1) Confidentiality Target Attacks (CTA): The paper[29] proposed a privacy-preserving scheme and a light-weighted lattice-based homomorphic encryption system which is mainly used to secure the amount of electricity consumed aggregate operation for home area networks. Results proved that the consumers' security and privacy is guaranteed with confidentiality, integrity, also computation overhead is reduced.

In [30], a methodology based on fog computing model is proposed to present a privacy-preserving and efficient scheme by making use of a cryptosystem that has a double trapdoor and aggregating the electricity usage by using fog nodes. Results show that the proposed method outperforms in terms of security objectives.

In this paper[45], a privacy preserving data aggregation scheme is proposed by using Boneh-Goh-Nissim public key cryptography to act against internal attacks in the smart grid system and thus, it achieved to ensure security of the smart grid system.

2) Integrity Attacks: This paper[31] presented about data integrity attacks that occurs online by designing an online attack strategy where the adversary does not have any idea about network data. Results showed that fair quantity of revenues through these attacks had generated by proposing an online countermeasure to detect these attacks and safeguard the system.

In this paper[32], a relaxing countermeasure is proposed to reduce the negative impact of these attacks and developed a control algorithm and sensitivity quantify attack signal and detection algorithm based on the CUSUM approach. What's more, they identify the false alarm by measuring the trade-off between the detection time and frequencies.

- False Data Injection Attacks: The paper [33] proposed a real-time, deep-learning approach to identify the behavior of the FDI in the intelligent voltage controller in the smart grid station, based on deep learning to address the identification of a complex statistical data structure using the Deep Belief Network (DBN) to capture temporal characteristics that have a high dimensionality.
  The article [34] proposed an adaptive Markov strategy to identify attacks that have an unpredictable nature in the smart grid systems. They also identified the behavior of false data injection into intelligent voltage controller, which can affect the overall microgrid performance.
  In this paper[35], an online algorithm was developed for anomaly detection based on load forecasting and synchrophasor data. The algorithm is independent from SCADA approach, to measure stealthy attack by gathering the variation of statistical data to predict the anomalous behavior between SCADA state estimate and forecasting prediction.
  The paper[36] concentrate on anomaly detection in context of EMS and DMS that can be occurred due to changes in topological and configuration of the database in form of false data injection. Multi varied time series model was introduced to examine the linear interrelationship between multiple time series. In paper [37], they addressed the problem on time series and network analysis package in anomaly detection method in industrial control system. This approach depends on characterizing the false data injection as binary classification problem by giving a promising outcome in the experiment set up as their dataset can be manually configured in various scenarios.
  In paper[16], the authors proposed a statistical anomaly detection technique based on the mixture Gaussian model. The proposed model is compared with the other techniques like BDD and machine learning algorithms like SVM, artificial neural networks.
  In this paper [38], two types of machine learning techniques were used. First one is the Conventional Bad Data Detection (BDD) technique to detect the false data that has been inserted due to abnormal sensors or like topological errors. Second detection technique is the Support Vector Machine that is used to detect the stealthy false insertions, with a given threshold value. PCA is used to reduce the dimensionality and Gaussian density function is applied.
  This paper[46] proposed an early online cyber-attack detection model based on partially observable Markov decision framework (POMDPs) and model-free reinforcement learning to detect attacks in timely manner. This framework makes detection model effective using zero-day attack, because the approach depends on reinforcement learning and cause the model to observe the data and map it to action.
  In this paper [47], the error tolerance of false data injection attacks have been analyzed by using a generalized linear measurement model to handle the smart grid monitoring devices like PMU and SCADA systems. But the drawback of this method is that, it cannot distinguish between different attacks.
  In [48] a statistical outlier detection technique was proposed by using S-estimator that was defined as a robust regression estimator that is implemented on the extended Kalman filter to capture the dynamic state of power systems. The S-Estimator is mainly introduced to improve accuracy and efficiency under cleaned data.
  This paper, [49] presented the most powerful statistical tool called as maximum likelihood estimator to detect false data injection attacksby utilizing chordal sparsity using modified Newton's method. This process guaranteed the privacy and security of the utilities by avoiding the data sharing between specific regions.

- Data Falsification Attacks: This paper [17] mainly concentrated on the false data that were produced by power consumption in advanced metering infrastructure. In order to detect these attacks, a statistical based anomaly detection technique is implemented by using threshold, which is calculated by using k-means clustering. In addition to that, Kullback-Leibler divergence trust model is utilized to detect the additive and deductive attacks of power consumption.

For extending the trust model, a generalized linear model with Weibull function, which is based on kernel trick is used for classifying the compromised nodes that has a chance of behaving anomalous and to detect the camouflage and conflict attacks. In this paper[39], an anomaly detection method is proposed to detect the blind and stealthy false data attacks. The performance showed the approximate result in detecting the blind false data attacks.

3) Availability Target Attacks (ATA): List of newly proposed availability target attacks like Denial-of-Service and Distributed Denial-of-Service attacks and their proposed anomaly detection techniques are described as follows:

- Denial-of-Service Attack: In this paper[40], anomaly detection was made on home area network (HAN) to detect cyber-attacks like flooding, which can cause the Denial of Service (DoS) in the smart grid networks. The authors of this paper used an unsupervised machine learning technique known as k-means clustering algorithm by grouping the data to form k number of clusters. The anomalies will be detected if any particular data object is absent in any clusters.
  This article[41] proposed an intrusion detection framework to detect the DoS attack called as Minimally Invasive Attack Mitigation via Detection Isolation and Localization (MIAMI-DIL) which employs an inference statistical model that is scalable in high dimensional data. This framework consists of detection stages, which is responsible for gathering data and statistics from the network and utilizes the intrusion detection system (IDS).
  This paper [42] proposed a framework, which controls and safeguards the cyber-physical system to improve the resilience. Depending on the delay in communication, the proposed model adapts its parameters. In order to enhance the time-delay tolerance, a delay-adaptive design is implemented to act against the cyber and physical attacks.
- Distributed Denial-of-Service Attack: The paper[43] studied the distributed denial of service attack (DDOS) in The AMI using honeypot-based approach known as Bayesian honeypot game model. This approach helped in increasing the level of detection as well as save energy consumption.

4) Cyber-Physical Attacks: In this paper [50], an intelligent remedial action scheme is a framework, which is also referred as special protection scheme, a decision tree-based anomaly detection algorithm is employed for differentiate between malicious tripping attack on relays and normal tripping due to power line faults. This model also performs the automatic correction based on the classification implemented and used decision tree rules to detect the anomalies and correct them.

This paper [51] studied new form of attack in smart grid called coordinated cyber -physical attack (CCPA) to detect power outage in terms of physical attack as well as sneakiness nature of cyber-attack. A defendant measure has been proposed to cover these two attacks by introducing a 4-bus power system and utilizing IEEE test power system. This paper[52] implemented a joint line removing and maintaining attack strategy that can mislead the control center by disconnecting the transmission line physically and increase the chance of cascading failures.

VI. New Lessons Learned

The electric grid becomes smart by providing a two-way communication between the utilities and the consumers. During the communication process, two types of threats may occur and effect the entire smart grid system. They are physical and cyber attacks and various types of sub attacks are explained. The main focus is on false data injection attack in cyber threats. In related work, the anomaly detection techniques that were proposed before 2015 were discussed. In this paper, new types of anomaly detection techniques that were proposed from 2016 to till now and explained how these techniques performs as defense strategies and protect the system against these attacks. In addition to that, many solutions adopt Hadoop and map-reduce techniques as real-time anomaly detection in smart grid. However, Hadoop and map-reduce techniques consider patch processing to store the data in a file and process it. It will be more beneficial if real-time data processing is used such as spark real-time data processing.

VII. Conclusion and Future Work

In this survey, different types of attacks and their anomaly detection techniques are explained in detail. Overall performance of the proposed techniques reached above 90 percent in successfully detecting these attacks and protecting the system. These techniques also ensured the security of the smart grid system with better accurate results.

For future work, we want to explore more on cyber-physical attacks and the defense strategies to protect the system from the cyber-physical attacks and study the performance of anomaly detection techniques especially when multiple types of malicious attacks occur at once to attack the smart grid system.

Acknowledgement

We would like to thank Dr. Satya Jayant Misra, Professor in Computer Science department at New Mexico State University for supporting us all the way in writing the survey project on anomaly detection in Smart Grid.

References

[1] What is Smart Grid?

[2] Mustafa A. Mustafa. *Smart Grid Security: Protecting Users'Privacy in Smart Grid Applications*. PhD thesis, 10 2015.

[3] X. Fang, S. Misra, G. Xue, and D. Yang. Smart grid — the new and improved power grid: A survey. *IEEE Communications Surveys Tutorials*, 14(4):944–980, 2012.

[4] L. Kotut and L. A. Wahsheh. Survey of cyber security challenges and solutions in smart grids. In *2016 Cybersecurity Symposium (CYBERSEC)*, pages 32–37, 2016.

[5] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, and A. R. Al Ali. Smart grid cyber security: Challenges and solutions. In *2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*, pages 170–175, 2015.

[6] S. S. S. Rawat, V. A. Polavarapu, V. Kumar, E. Aruna, and V. Sumathi. Anomaly detection in smart grid using rough set theory and k cross validation. In *2014 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2014]*, pages 479–483, 2014.

[7] L. Yang and F. Li. Detecting false data injection in smart grid in-network aggregation. In *2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 408–413, 2013.

[8] A. M. Kosek. Contextual anomaly detection for cyber-physical security in smart grids based on an artificial neural network model. In *2016 Joint Workshop on Cyber- Physical Security and Resilience in Smart Grids (CPSR-SG)*, pages 1–6, 2016.

[9] O. Linda, M. Manic, and T. Vollmer. Improving cyber-security of smart grid systems via anomaly detection and linguistic domain knowledge. In *2012 5th International Symposium on Resilient Control Systems*, pages 48–54, 2012.

[10] Shubhalaxmi Kher, Victor Nutt, Dipankar Dasgupta, Hasan Ali, and Paul Mixon. A prediction model for anomalies in smart grid with sensor network. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, CSIIRW '13, New York, NY, USA, 2013. Association for Computing Machinery.

[11] M. Levorato and U. Mitra. Fast anomaly detection in smartgrids via sparse approximation theory. In *2012 IEEE 7th Sensor Array and Multichannel Signal Processing Workshop (SAM)*, pages 5–8, 2012.

[12] Y. Yuan and K. Jia. A distributed anomaly detection method of operation energy consumption using smart meter data. In *2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, pages 310–313, 2015.

[13] Z. A. Baig. On the use of pattern matching for rapid anomaly detection in smart grid infrastructures. In *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 214–219, 2011.

[14] J. Wu, J. Xiong, P. Shil, and Y. Shi. Real time anomaly detection in wide area monitoring of smart grids. In *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pages 197–204, 2014.

[15] X. Liu and Z. Li. Local topology attacks in smart grids. *IEEE Transactions on Smart Grid*, 8(6):2617–2626, 2017.

[16] S. A. Foroutan and F. R. Salmasi. Detection of false data injection attacks against state estimation in smart grids based on a mixture gaussian distribution learning method. *IET Cyber-Physical Systems: Theory Applications*, 2(4):161–171, 2017.

[17] Shameek Bhattacharjee, Aditya Thakur, Simone Silvestri, and Sajal K. Das. Statistical security incident forensics against data falsification in smart grid advanced metering infrastructure. In *Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy*, CODASPY '17, page 35–45, New York, NY, USA, 2017. Association for Computing Machinery.

[18] What is a DDoS Attack?

[19] M. Ghanbari, W. Kinsner, and K. Ferens. Anomaly detection in a smart grid using wavelet transform, variance fractal dimension and an artificial neural network. In *2016 IEEE Electrical Power and Energy Conference (EPEC)*, pages 1–6, 2016.

[20] K. Candelario, C. Booth, A. St.Leger, and S. J. Matthews. Investigating a raspberry pi cluster for detecting anomalies in the smart grid. In *2017 IEEE MIT Undergraduate Research Technology Conference (URTC)*, pages 1–4, 2017.

[21] S. J. Matthews and A. St. Leger. Leveraging mapreduce and synchrophasors for real-time anomaly detection in the smart grid. *IEEE Transactions on Emerging Topics in Computing*, 7(3):392–403, July 2019.

[22] S. J. Matthews and A. St. Leger. Leveraging mapreduce and synchrophasors for real-time anomaly detection in the smart grid. *IEEE Transactions on Emerging Topics in Computing*, 7(3):392–403, 2019.

[23] R. Moghaddass and J. Wang. A hierarchical framework for smart grid anomaly detection using large-scale smart meter data. *IEEE Transactions on Smart Grid*, 9(6):5820–5830, 2018.

[24] B. Rossi, S. Chren, B. Buhnova, and T. Pitner. Anomaly detection in smart grid data: An experience report. In *2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pages 002313–002318, 2016.

[25] Cristina Alcaraz, Lorena Cazorla, and Gerardo Fernandez. Context-awareness using anomaly-based detectors for smart grid domains. In Javier Lopez, Indrajit Ray, and Bruno Crispo, editors, *Risks and Security of Internet and Systems*, pages 17–34, Cham, 2015. Springer International Publishing.

[26] F. Passerini and A. M. Tonello. Smart grid monitoring using power line modems: Anomaly detection and localization. *IEEE Transactions on Smart Grid*, 10(6):6178–6186, 2019.

[27] G. Fenza, M. Gallo, and V. Loia. Drift-aware methodology for anomaly detection in smart grid. *IEEE Access*, 7:9645–9657, 2019.

[28] J. Pereira and M. Silveira. Unsupervised anomaly detection in energy time series data using variational recurrent autoencoders with attention. In *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pages 1275–1282, 2018.

[29] A. Abdallah and X. S. Shen. A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid. *IEEE Transactions on Smart Grid*, 9(1):396–405, 2018.

[30] J. Liu, J. Weng, A. Yang, Y. Chen, and X. Lin. Enabling efficient and privacy-preserving aggregation communication and function query for fog computing-based smart grid. *IEEE Transactions on Smart Grid*, 11(1):247–257, 2020.

[31] S. Tan, W. Song, M. Stewart, J. Yang, and L. Tong. Online data integrity attacks against real-time electrical market in smart grid. *IEEE Transactions on Smart Grid*, 9(1):313–322, 2018.

[32] J. Giraldo, A. Cárdenas, and N. Quijano. Integrity attacks on real-time pricing in smart grids: Impact and countermeasures. *IEEE Transactions on Smart Grid*, 8(5):2249–2257, 2017.

[33] Y. He, G. J. Mendis, and J. Wei. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. *IEEE Transactions on Smart Grid*, 8(5):2505–2516, 2017.

[34] J. Hao, E. Kang, J. Sun, Z. Wang, Z. Meng, X. Li, and Z. Ming. An adaptive markov strategy for defending smart grid false data injection from malicious attackers. *IEEE Transactions on Smart Grid*, 9(4):2398–2408, 2018.

[35] A. Ashok, M. Govindarasu, and V. Ajjarapu. Online detection of stealthy false data injection attacks in power system state estimation. *IEEE Transactions on Smart Grid*, 9(3):1636–1646, 2018.

[36] A. Anwar, A. N. Mahmood, and Z. Tari. Ensuring data integrity of opf module and energy database by detecting changes in power flow patterns in smart grids. *IEEE Transactions on Industrial Informatics*, 13(6):3299–3311, 2017.

[37] C. Feng, T. Li, and D. Chana. Multi-level anomaly detection in industrial control systems via package signatures and lstm networks. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 261–272, 2017.

[38] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han. Detecting stealthy false data injection using machine learning in smart grid. *IEEE Systems Journal*, 11(3):1644–1652, 2017.

[39] W. Chin, C. Lee, and T. Jiang. Blind false data attacks against ac state estimation based on geometric approach in smart grid communications. *IEEE Transactions on Smart Grid*, 9(6):6298–6306, 2018.

[40] D. M. Menon and N. Radhika. Anomaly detection in smart grid traffic data for home area network. In *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, pages 1–4, 2016.

[41] Y. Yilmaz and S. Uludag. Mitigating iot-based cyberattacks on the smart grid. In *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pages 517–522, 2017.

[42] A. Farraj, E. Hammad, and D. Kundur. A cyber-physical control framework for transient stability in smart grids. *IEEE Transactions on Smart Grid*, 9(2):1205–1215, 2018.

[43] K. Wang, M. Du, S. Maharjan, and Y. Sun. Strategic honeypot game model for distributed denial of service attacks in the smart grid. *IEEE Transactions on Smart Grid*, 8(5):2474–2482, 2017.

[44] Yu Kang, Xinting Wang, Xiu Cao, Yangfan Zhou, Zhichao Lai, Yuhao Li, Xuqi Zhang, and Wei Geng. Detecting anomalous users via streaming data processing in smart grid. In *Proceedings of the 2018 International Conference on Mechatronic Systems and Robots*, ICMSR '18, page 14–20, New York, NY, USA, 2018. Association for Computing Machinery.

[45] D. He, N. Kumar, S. Zeadally, A. Vinel, and L. T. Yang. Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries. *IEEE Transactions on Smart Grid*, 8(5):2411–2419, 2017.

[46] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang. Online cyber-attack detection in smart grid: A reinforcement learning approach. *IEEE Transactions on Smart Grid*, 10(5):5174–5185, 2019.

[47] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, and J. Wang. Short-term state forecasting-aided method for detection of smart grid general false data injection attacks. *IEEE Transactions on Smart Grid*, 8(4):1580–1590, 2017.

[48] Y. Chakhchoukh, H. Lei, and B. K. Johnson. Diagnosis of outliers and cyber attacks in dynamic pmu-based power state estimation. *IEEE Transactions on Power Systems*, 35(2):1188–1197, 2020.

[49] R. Moslemi, A. Mesbahi, and J. M. Velni. A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids. *IEEE Transactions on Smart Grid*, 9(5):4930–4941, 2018.

[50] V. K. Singh and M. Govindarasu. Decision tree based anomaly detection for remedial action scheme in smart grid using pmu data. In *2018 IEEE Power Energy Society General Meeting (PESGM)*, pages 1–5, 2018.

[51] R. Deng, P. Zhuang, and H. Liang. Ccpa: Coordinated cyber-physical attacks and countermeasures in smart grid. *IEEE Transactions on Smart Grid*, 8(5):2420–2430, 2017.

[52] H. Chung, W. Li, C. Yuen, W. Chung, Y. Zhang, and C. Wen. Local cyber-physical attack for masking line outage and topology attack in smart grid. *IEEE Transactions on Smart Grid*, 10(4):4577–4588, 2019.